الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي و البحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة أبي بكر بلقايد- تلمسان -

Université AboubakrBelkaïd– Tlemcen –
Faculté de TECHNOLOGIE

MEMOIRE

Présenté pour l'obtention du **diplôme** de **MASTER**

En : Télécommunication

Spécialité : Télécommunications Optiques

Par :

BOUHASSANE Radja
&
NASSOUR Boumedien Habib Allah

Sujet

Crypto-Système Chaotique à double retard utilisant des modulateurs Mach-Zehnder pour la sécurisation des Communications Optiques Haut Débits

Soutenu publiquement, le 30/06/2025, devant le jury composé de :

M BOUABDALLAH Reda	MCB	Université de Tlemcen	Président
Mme OTMANI Amina	MCB	Université de Tlemcen	Examinateur
M ABDELMALEK Abdelhafid	MCB	Université de Tlemcen	Encadreur
Mme SLIMANE Zohra	Professeur	Université de Tlemcen	Co-Encadreur

Année universitaire : 2024/2025

Remerciements

Avant toute chose, nous rendons grâce à ALLAH, le Tout-Puissant, pour nous avoir permis de mener à terme ce travail avec force, patience et sérénité.

Nous tenons à exprimer notre profonde reconnaissance à Monsieur Abdelmalek Abdelhafid Maître de conférences de l'Université de Tlemcen et Mme Slimane Zohra Professeur de l'Université de Tlemcen, pour avoir accepté de nous encadrer et pour nous avoir confié ce sujet de recherche, riche et formateur.

Leur implication, leur guidance méthodique, ainsi que leur écoute attentive nous ont été d'un grand soutien tout au long de l'élaboration de ce travail. Grâce à leur accompagnement rigoureux et leurs orientations éclairées, nous avons pu avancer sereinement, acquérir de solides bases en recherche scientifique, et mener ce projet à bien dans un cadre de travail stimulant et bienveillant.

Nous exprimons notre profonde reconnaissance à Monsieur Bouabdallah Reda de Maître de conférences de l'Université de Tlemcen, pour avoir accepté de présider le jury de notre mémoire, et pour l'honneur qu'il nous fait par sa présence.

Nous remercions également Mme Otmani Amina, Maître de conférences au sein de la même université, pour avoir accepté d'évaluer notre travail et pour l'attention bienveillante portée à notre recherche.

Nous souhaitons adresser nos remerciements les plus sincères à nos familles, pour leur soutien inestimable, leur présence réconfortante et leurs encouragements constants, qui nous ont accompagnés à chaque étape de notre formation. Leur confiance et leur bienveillance ont été, pour nous, une source de motivation inépuisable.

Nos pensées vont également à nos camarades de promotion, avec qui nous avons partagé des efforts, des doutes et des réussites. Leur esprit d'équipe, leur générosité et leur bonne humeur ont marqué positivement cette expérience universitaire.

Dédicaces

Je dédie ce travail avec beaucoup d'amour à :

Mes chers parents

Ma mère "Rabia" et mon père "Ahmed" pour leur soutien indéfectible, leur patience infinie et leur confiance en moi. Leur présence et leurs sacrifices ont été le fondement de mon parcours.

Mes chers frères "Ali" et "Akram"

Ma grand-mère et mon grand-père que le bon seigneur les garde pour nous

Mes chers oncles, Mes chers tantes, Mes chers cousines et à tout ma famille

Mes belles copines "Wafaa, Besma, Amina, Achwak, Ghizlen et Ghozlen" et tous mes amis

A mon binôme "Habib Allah" pour ta collaboration précieuse, ton sérieux et ton engagement tout au long de ce travail.

A tout ma promotion Télécommunications Optiques 2023/2025

A mes enseignants devant mon primaire jusqu'à maintenant

Radja

Dédicaces

Je dédie ce Modest travail à ma famille, elle qui m'a doté d'une éducation digne, son amour a fait de moi ce que je suis aujourd'hui :

Particulièrement à mon père "Miloud" et ma mère "Badia"

A vous mes frères "Djad" et "Iyad" et mes sœurs "Rihem" et "Tesnim" qui m'avais toujours soutenu et encouragé durant ces années d'études.

A ma chère binôme "Radja", et à tous mes collègues de la promotion master 2 Télécommunication Optique.

"Habib"

Résumé

Dans ce mémoire, nous avons conçu et étudié un crypto-système chaotique sécurisé basé sur l'utilisation de deux modulateurs Mach-Zehnder (MZM) intégrés dans une architecture à double retard. Ce système repose sur une dynamique électro-optique non linéaire introduite par les modulateurs MZM, permettant de générer un comportement chaotique complexe et de haute dimension.

Le système se compose de deux parties principales : l'émetteur, qui regroupe le générateur de chaos optique et le module de chiffrement, et le récepteur, comprenant les modules de synchronisation et de déchiffrement. Le modèle mathématique établi décrit une équation différentielle non linéaire à retard, tenant compte des deux branches de modulation. Nous avons mené une étude numérique sous MATLAB, dans laquelle nous avons analysé les effets des paramètres de gain et de retard sur la dynamique du système.

Les résultats obtenus à travers les réponses temporelles, diagrammes de bifurcation et plans de phase ont permis d'identifier les zones où le système présente un comportement périodique, quasi-périodique ainsi chaotique. Le signal chaotique généré a ensuite été utilisé pour le chiffrement optique par modulation d'intensité, et l'ensemble du processus de chiffrement/déchiffrement a été validé sous l'environnement OptiSystem, à l'aide des signaux simulés dans MATLAB.

Ce travail met ainsi en évidence la faisabilité et la performance d'un système de communication sécurisé fondé sur le chaos optique multi-modulateur, et souligne les avantages d'une configuration à double MZM pour renforcer la complexité du signal et la robustesse du crypto-système.

Mots clés : Chaos, bifurcation, Exposant de Lyapunov, Attracteur étrange, stabilité, cascade sous harmonique, quasi-périodicité, Dimension fractale, modulateur Mach Zhender, équation différentielle à retard, Runge Kutta, non linéaire, Synchronisation, Matlab, Optisystem.

Abstract

In this memoir , we designed and studied a secure chaotic cryptosystem based on the use of two Mach-Zehnder modulators (MZMs) integrated into a double-delay architecture. This system relies on the nonlinear electro-optical dynamics introduced by the MZMs, allowing for the generation of complex, high-dimensional chaotic behavior.

The system consists of two main parts: the transmitter, which includes the optical chaos generator and the encryption module, and the receiver, which contains the synchronization and decryption modules. The developed mathematical model describes a delayed nonlinear differential equation that accounts for both modulation branches. A numerical study was conducted using MATLAB, analyzing the effects of gain and delay parameters on the system's dynamics.

The results, obtained through time-domain responses, bifurcation diagrams, and phase portraits, helped identify the regions where the system exhibits periodic, quasi-periodic, and chaotic behavior. The generated chaotic signal was then used for optical encryption via intensity modulation, and the full encryption/decryption process was validated in the OptiSystem environment using MATLAB-simulated signals.

This work highlights the feasibility and performance of a secure communication system based on multi-modulator optical chaos, and emphasizes the advantages of a double-MZM configuration in increasing signal complexity and system robustness.

Keywords: Chaos, bifurcation, Lyapunov exponent, strange attractor, stability, subharmonic cascade, quasi-periodicity, fractal dimension, Mach-Zehnder modulator, delay differential equation, Runge-Kutta, nonlinear, synchronization, MATLAB, OptiSystem.

ملخص

في هذه المذكرة ، قمنا بتصميم ودراسة نظام تشفير فوضوي آمن يعتمد على استخدام مُعدِّلَيْ ماخ-زيندر (MZM) مُدمَجَيْن في بنية ذات تأخير مزدوج. يعتمد هذا النظام على ديناميكية كهروبصرية غير خطية تُحدِثها مُعدِّلات ماخ-زيندر، مما يسمح بتوليد سلوك فوضوي معقد وعالي الأبعاد.

يتكون النظام من جزأين رئيسيين: المرسِل، الذي يضم مولِّد الفوضى الضوئية ووحدة التشفير، والمستقبِل، الذي يشمل وحدات التزامن وفك التشفير. يصف النموذج الرياضي المُنشأ معادلة تفاضلية غير خطية ذات تأخير، مع الأخذ في الاعتبار فرعي التعديل. أجرينا دراسة عددية باستخدام برنامج MATLAB ، قمنا فيها بتحليل تأثيرات معاملي الكسب والتأخير على ديناميكية النظام.

أتاحت النتائج التي تم الحصول عليها من خلال الاستجابات الزمنية، ومخططات التشعب، ومستويات الطور، تحديد المناطق التي يُظهر فيها النظام سلوكًا دوريًا، وشبه دوري، وفوضوي. بعد ذلك، تم استخدام الإشارة الفوضوية المولَّدة في التشفير الضوئي عن طريق تعديل الشدة، وتم التحقق من صحة عملية التشفير وفك التشفير بأكملها في بيئةOptiSystem، باستخدام الإشارات التي تمت محاكاتها في.MATLAB

وبهذا، يُبرز هذا العمل جدوى وأداء نظام اتصالات آمن قائم على الفوضى الضوئية متعددة المعدِّلات، ويؤكد على مزايا استخدام تكوين مزدوج لمُعدِّلات ماخ-زيندر لتعزيز تعقيد الإشارة ومتانة نظام التشفير.

الكلمات المفتاحية: "نظام فوضوي، التفرع، مؤشر ليابونوف، الجاذب الغريب، الاستقرار، سلسلة التوافقات الجزئية، شبه الدورية، البُعد الكسري، معدل ماخ-زيندر، معادلة تفاضلية مع تأخير، رونج-كوتا، غير خطي، التزامن، ماتلاب، أوبتي سيستم".

Table des matières

Chapitre II

Techniques de chiffrement chaotique

Chapitre III

Evaluation des performances d'un crypto-système chaotique basé sur MZM

Liste des Figures

Chapitre I

Chapitre II

Chapitre III

Liste des Tableaux

Chapitre I

Chapitre III

Introduction Générale

Dans un monde où les échanges d'informations sensibles sont devenus omniprésents et instantanés, À l'ère des communications numériques, les fibres optiques forment la colonne vertébrale des réseaux de télécommunications modernes, grâce à leur capacité à transporter de grandes quantités d'informations à très haute vitesse. La sécurité des communications représente aujourd'hui un enjeu stratégique de premier ordre, que ce soit dans les domaines civils, militaires, industriels ou institutionnels. Toutefois, les méthodes de chiffrement classiques, fondées sur des algorithmes mathématiques tels que AES, DES, RSA, DSA, ElGamal ou ECC, montrent leurs limites en matière de performances, notamment lorsqu'il s'agit de répondre aux exigences des communications à très haut débit qui se provoque un problème dans le domaine optique. Dans ce contexte, la cryptographie chaotique émerge comme une alternative prometteuse aux techniques conventionnelles, en exploitant les propriétés complexes des systèmes dynamiques non linéaires pour générer des signaux hautement imprévisibles et difficilement reproductibles. [1]

Le présent travail s'inscrit dans cette dynamique. Il porte sur la conception, l'étude et la simulation d'un crypto-système chaotique à double retard, basé sur l'utilisation de deux modulateurs Mach-Zehnder (MZM), dans le but de sécuriser la transmission de données optiques à haut débit. Ce type de système exploite la génération de chaos optique contrôlé et la synchronisation entre émetteur et récepteur pour dissimuler efficacement le signal d'information.

Ce mémoire est structuré en trois chapitres. Le premier est consacré à un état de l'art sur les systèmes dynamiques chaotiques, où nous exposons les notions fondamentales et les propriétés clés de ces systèmes. Le second chapitre aborde les bases du chiffrement chaotique, avec une présentation des principales techniques de cryptage fondées sur le chaos. Enfin, le troisième chapitre représente le cœur de notre contribution. Il est dédié à la mise en œuvre, à l'analyse et à l'évaluation de notre approche proposée :

- Élaborer un émetteur reposant sur un générateur chaotique.
- Définir les équations mathématiques qui régissent le modèle.
- Étudier l'évolution chaotique induite par un paramètre donné.
- Représenter graphiquement les évolutions temporelles du système.
- Générer le diagramme de bifurcation pour analyser les régimes dynamiques du système.

Les différentes simulations et analyses numériques ont été réalisées à l'aide des environnements MATLAB et OptiSystem, afin de modéliser le comportement du système et d'évaluer ses performances .[2]

Chapitre I

Systèmes dynamiques chaotiques

I.1 Introduction

Les systèmes dynamiques chaotiques forment une classe spéciale de systèmes dynamiques qui se caractérisent par une sensibilité élevée aux conditions initiales et un comportement imprévisible, bien que ceux-ci soient déterministes. Leur étude a été menée depuis plusieurs décennies en raison de l'intérêt dans divers domaines scientifiques et technologiques, tels que la physique, la biologie, l'ingénierie et la cryptographie. Ce chapitre présente les concepts de base des systèmes dynamiques, en distinguant entre des systèmes continus et discrets, pour définir ensuite les propriétés des systèmes chaotiques. Ensuite, il offre une analyse des outils mathématiques utilisés pour l'analyse de leur comportement et les applications de ces systèmes pour la sécurisation des communications optiques.

I.2 Systèmes Dynamiques

I.2.1 Définition

Un système dynamique est un modèle mathématique qui décrit l'évolution d'un état au cours du temps en fonction d'une règle bien définie. Il est caractérisé par un ensemble d'équations qui régissent la transformation de l'état du système sous l'effet du temps.[3]

L'analyse de l'évolution d'un système repose sur deux éléments essentiels :

- **Son état initial**, qui correspond à sa condition à l'instant t_0.
- **Sa loi d'évolution**, qui détermine la manière dont il évolue au fil du temps.

Les systèmes dynamiques sont classés en plusieurs catégories (systèmes continus, discrets, autonomes, non autonomes, linéaires et non linéaires). Ces systèmes sont largement utilisés en physique, biologie, économie, ingénierie et bien d'autres domaines pour modéliser des phénomènes dynamiques tels que la mécanique des fluides, la dynamique des populations, les circuits électriques, ou encore les systèmes chaotiques. [4,3]

I.2.2 Types de systèmes dynamiques

I.2.2.1 *Système continu*

Un système dynamique continu évolue de manière fluide sans interruptions. Mathématiquement, un système dynamique continu est souvent représenté sous la forme :

$$\frac{dx}{dt} = f(x,t)$$

Où :

- X représente l'état du système à un instant donné.
- T est la variable temporelle.
- F (x, t) est une fonction qui régit l'évolution de x. [4 ,5]

I.2.2.2 *Système discret*

Un système dynamique discret est contrairement aux systèmes continus, il évolue à des instants distincts (discrets) plutôt que de manière continue. Souvent modélisé par des équations de récurrence. [5]

Mathématiquement, un système dynamique discret est décrit par une relation de récurrence de la forme :

$$x_{n+1} = f(x_n, n)$$

Où :

- x_n représente l'état du système à l'instant n.
- n est un entier représentant le temps discret.[5]

I.2.2.3 *Système autonome vs non autonome*

- ***Système autonome***

Un système dynamique autonome est un système dont l'évolution dépend uniquement de son état actuel, sans dépendance explicite au temps. Autrement dit, la loi d'évolution du système

reste invariante dans le temps. Il est généralement décrit par des équations différentielles de la forme :

$$\frac{dx}{dt} = f(x)$$

Où x est le vecteur des variables d'état, et f est une fonction définissant la dynamique du système. [6]

Caractéristiques d'un Système Autonome

1. **Indépendance temporelle** : L'évolution ne change pas en fonction de l'instant où elle est observée.
2. **Présence d'équilibres** : Il peut exister des points fixes x* où$f(x^*) = 0$, indiquant des états stables ou instables.
3. **Conservation des trajectoires** : Pour un même état initial, le système suivra toujours la même trajectoire indépendamment de l'instant où il commence. [4]

- ***Système non-autonome***

À l'inverse, un **système dynamique non autonome** est un système dont l'évolution dépend explicitement du temps, il est influencé par des facteurs externes variant avec le temps. Il est décrit par des équations différentielles de la forme :

$$\frac{dx}{dt} = f(x, t)$$

Où x représente le vecteur des variables d'état, t le temps.

Caractéristiques d'un Système Non Autonome

1. **Dépendance explicite au temps** : La loi d'évolution varie en fonction de t.
2. **Influence des forces extérieures** : Souvent, un terme extérieur (comme une force ou un signal) modifie le comportement du système.

3. **Absence d'invariance temporelle** : Si l'on change l'instant initial, l'évolution du système peut être différente. [4]

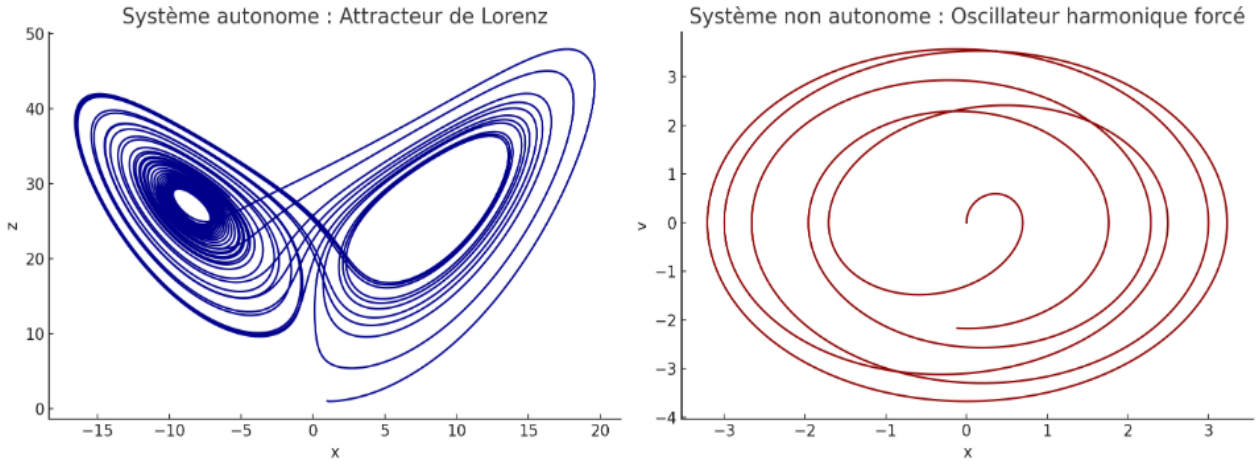

Figure I.1:Exemple d'un système autonome et non autonome

I.3 Systèmes chaotiques

Le phénomène du chaos se manifeste dans des systèmes dynamiques non linéaires complexes, caractérisés par une dépendance sensible aux conditions initiales. Dans ces systèmes, les trajectoires évoluent au sein d'une région bornée de manière stable, sans toutefois converger vers un point fixe ou un cycle limite. Ces trajectoires, qui demeurent denses dans cette région, sont extrêmement sensibles aux conditions de départ. Les équations différentielles non linéaires décrivant ces systèmes ne possèdent généralement pas de solutions analytiques exactes, sauf pour certaines classes particulières. Par conséquent, leurs solutions sont souvent déterminées numériquement, et le comportement du système est analysé par des simulations. Le terme "chaos", associé aux applications itérées, a été formellement introduit par Li et Yorke en 1975, lorsqu'ils ont établi un critère simple pour identifier le chaos dans les équations aux différences unidimensionnelles.

Le chaos ne peut émerger, dans un système dynamique continu, que si celui-ci est décrit par au moins trois variables d'état indépendantes. [7,3]

I.3.1 Principales caractéristiques du chaos

Il existe plusieurs caractéristiques du chaos tels que

I.3.1.1 *Non-linéarité*

Un système chaotique correspond à un système dynamique de nature non linéaire. À l'inverse, un système linéaire ne peut pas présenter un comportement chaotique. Ce caractère chaotique résulte généralement des non-linéarités présentes dans le modèle. Pour étudier et anticiper les phénomènes produits par un système dynamique, on élabore en général un modèle mathématique qui relie les causes aux effets. Lorsque cette relation est proportionnelle, le système est dit linéaire. En revanche, dans un système non linéaire, les effets ne varient pas de manière proportionnelle aux causes, ce qui introduit une complexité pouvant mener à un comportement chaotique. [8]

I.3.1.2 *Déterministe*

Le déterminisme implique que, connaissant l'état initial d'un phénomène à un moment donné, il est théoriquement possible de prévoir son évolution future. Dans le contexte des systèmes chaotiques, qui sont souvent décrits par des équations différentielles non linéaires, cette prévisibilité est limitée. En effet, bien que ces équations définissent précisément le comportement dynamique du système, la sensibilité extrême aux conditions initiales rend les prédictions à long terme très difficiles. De petites incertitudes ou erreurs dans la connaissance de l'état initial peuvent conduire à des divergences significatives dans l'évolution du système, illustrant ainsi le caractère imprévisible des systèmes chaotiques malgré leur nature déterministe. [9]

I.3.1.3 *Sensibilité aux conditions initiales*

La sensibilité aux conditions initiales, souvent désignée simplement par "sensitivité", est une caractéristique fondamentale des systèmes chaotiques. Elle a été mise en évidence pour la première fois par Edward Lorenz à travers ses travaux sur un modèle météorologique. Ce phénomène est aujourd'hui largement connu sous le nom « d'effet papillon ». Dans un système chaotique, une infime incertitude ou une légère variation dans la connaissance de l'état initial

$x_0$peut entraîner, avec le temps, des écarts considérables dans l'évolution du système, rendant toute prédiction à long terme extrêmement difficile. [10]

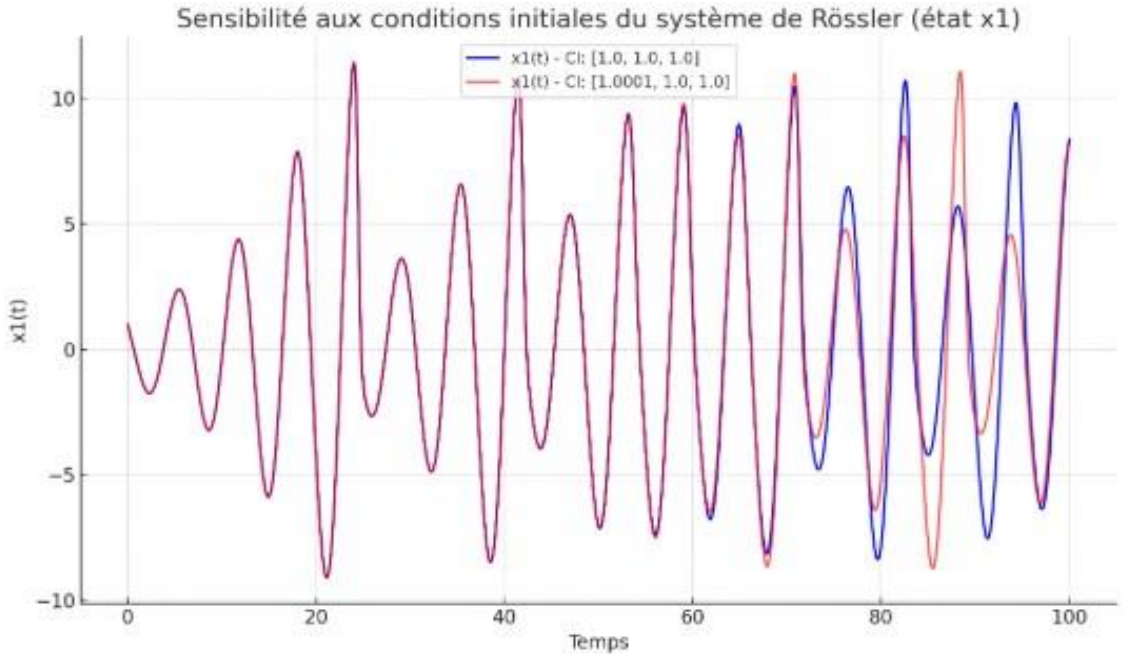

Figure I.2:Comparaison des trajectoires de x1 avec des conditions initiales proches, illustrant la dynamique chaotique du système de Rössler.

I.3.2 Outils mathématiques pour l'analyse des systèmes chaotiques

Il existe deux type des outils mathématiques pour l'analyse des systèmes chaotiques

I.3.2.1 *Qualitatif*

- **Espace de phase**

Un système dynamique est défini par un ensemble de variables d'état qui décrivent complètement son état à un instant donné. L'évolution temporelle de ces variables reflète le comportement dynamique du système. L'ensemble de toutes les valeurs possibles de ces variables constitue l'espace des phases, où chaque point représente un état spécifique du système. Le déplacement de ces points dans l'espace des phases au fil du temps trace des trajectoires, également appelées orbites, illustrant l'évolution du système. Il permet de transformer des séries de données numériques en une représentation géométrique, facilitant ainsi la visualisation de l'évolution du système. [11,12]

o Les Attracteurs

Un attracteur fait référence à un ensemble de points dans l'espace des phases vers lesquels les trajectoires convergent finalement au fil du temps, quelles que soient les conditions initiales proches. Selon le système dynamique étudié, cet attracteur peut se manifester sous différentes formes. Il peut s'agir d'un

→ **Point fixe :** indiquant que le système atteint une configuration stable.
→ **Cycle limite :** où le système subit des oscillations régulières.
→ **Un tore :** dans lequel les trajectoires suivent un chemin périodique dans un espace de dimension supérieure.

Ces constructions permettent de caractériser la dynamique asymptotique des systèmes, en particulier dans des contextes chaotiques où les trajectoires peuvent présenter une sensibilité aux conditions initiales tout en restant limitées à un ensemble spécifique dans l'espace des phases. [13]

- **Densité spectrale de puissance (DSP)**

La densité spectrale permet de caractériser la distribution de l'énergie au sein d'un signal sur différentes fréquences. Il s'avère particulièrement intéressant pour l'examen de signaux chaotiques, car il met en évidence l'existence d'un spectre à large bande, emblématique des systèmes non périodiques. Contrairement aux signaux périodiques qui présentent des pics distincts à certaines fréquences, les signaux chaotiques révèlent une distribution d'énergie continue, signe de leur complexité et de leur imprévisibilité. Par conséquent, l'analyse de la densité spectrale facilite la différenciation entre les comportements ordonnés et chaotiques, constituant une ressource inestimable dans des disciplines telles que la cryptographie, où l'objectif consiste souvent à générer des signaux difficiles à prévoir. [13]

I.3.2.2 *Quantitatif*

- **Exposants de Lyapunov**

Les exposants de Lyapunov quantifient la stabilité d'un système dynamique en mesurant la sensibilité aux conditions initiales. Ils évaluent le taux de divergence ou de convergence de

trajectoires proches dans l'espace des phases. Un exposant de Lyapunov positif indique une divergence exponentielle des trajectoires, caractéristique du comportement chaotique, tandis qu'un exposant négatif suggère une convergence vers des points fixes ou des cycles limites, reflétant une dynamique stable. Les systèmes linéaires présentent généralement des exposants de Lyapunov négatifs ou nuls, indiquant des mouvements bornés et stables. Dans les systèmes non linéaires, l'analyse des exposants de Lyapunov permet d'évaluer la stabilité locale autour des points d'équilibre et de déterminer la présence éventuelle de chaos. Cette sensibilité aux conditions initiales rend la prévision à long terme des systèmes chaotiques particulièrement complexe, car de petites perturbations peuvent entraîner des divergences significatives dans l'évolution du système. [14]

Dimension	Exposants de lyapunov	Etat
0	$\lambda n \leq \cdots . \leq \lambda 1 \leq 0$	Point d'équilibre
1	$\lambda 1 = 0\ ,\ \lambda n \leq \cdots . \leq \lambda 2 \leq 0$	Périodique
2	$\lambda 1 = \lambda 2 = 0\ ;\ \lambda n \leq \cdots . \leq \lambda 3 \leq 0$	Période d'ordre 2
K	$\lambda 1 = \cdots . = \lambda k = 0; \lambda n \leq \cdots .. \leq \lambda k + 1 \leq 0$	Quasi-périodique
Non Entier	$\lambda 1 > 0; \sum_{i+1}^{n} \lambda i < 0$	Chaotique
Non Entier	$\lambda 1 > 0\ ,\ \lambda 2 > 0; \sum_{i+1}^{n} \lambda i < 0$	Hyper-Chaotique

Tableau I.1: Exposants de Lyapunov

- **Diagramme de bifurcation**

Dans le cadre des systèmes dynamiques, un diagramme de bifurcation permet d'analyser les différents régimes de comportement qu'un système peut adopter à long terme en fonction de la variation d'un ou plusieurs paramètres appelés paramètres de bifurcation. Ce type de diagramme représente une région de l'espace des paramètres dans laquelle sont tracés les points où le système change qualitativement de comportement, marquant ainsi l'apparition de bifurcations. [15]

La figure ci-dessous nous montre un exemple de diagramme de bifurcation de la fonction logistique.

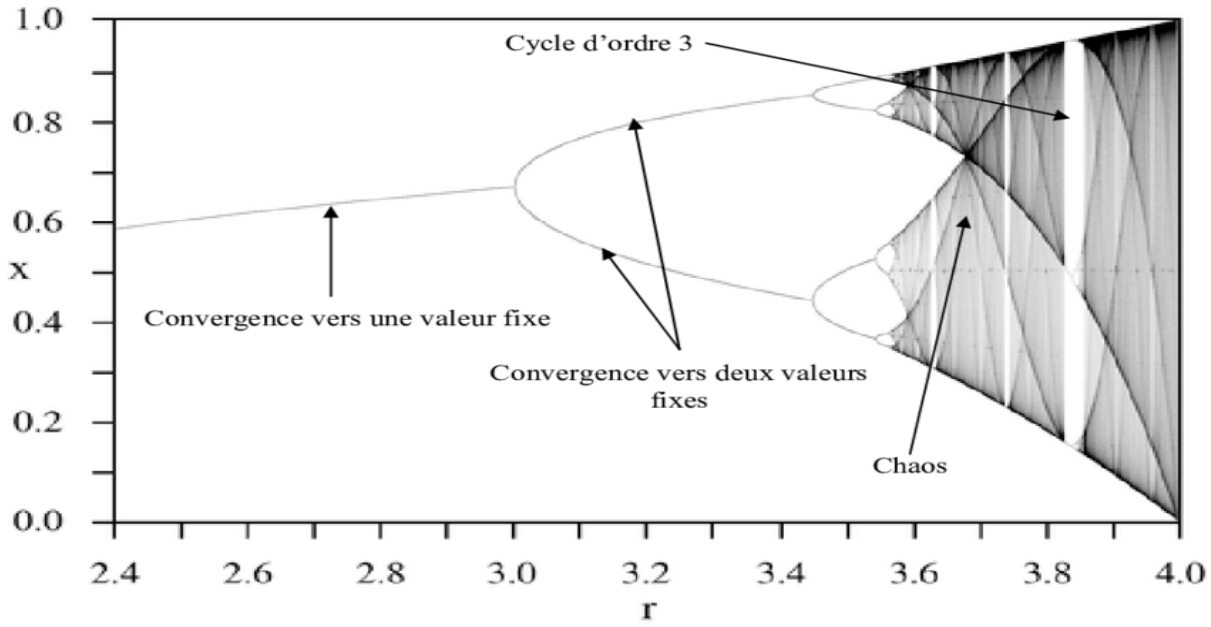

Figure I.3 : Diagramme de bifurcation pour un système chaotique.[9]

- **Dimension fractale**

Lors de l'examen des systèmes dynamiques chaotiques, les attracteurs étranges sont caractérisés par leur configuration géométrique complexe et erratique. Contrairement aux attracteurs simples tels que les points d'équilibre ou les cycles limites, les attracteurs étranges possèdent une dimension fractale, qui est une dimension non entière inférieure à celle de l'espace des phases. Cet attribut indique l'auto similitude et la concentration de l'attracteur dans l'espace des phases, démontrant ainsi la nature complexe des trajectoires chaotiques qui convergent dans cette région. Par exemple, l'attracteur de Rössler présente une structure

fractale, illustrant les caractéristiques particulières de certains attracteurs au sein de systèmes dynamiques non linéaires. [11]

I.4 Conclusion

Les systèmes dynamiques chaotiques représentent une branche essentielle des systèmes non linéaires, caractérisée par des comportements complexes et imprévisibles. Leur étude repose sur des outils mathématiques avancés, comme les exposants de Lyapunov, les attracteurs étranges et les diagrammes de bifurcation, qui permettent de mieux comprendre leur dynamique.

Grâce à leurs propriétés uniques, ces systèmes trouvent des applications dans de nombreux domaines, notamment en cryptographie, où ils sont exploités pour sécuriser les communications optiques à haut débit. Ce chapitre a permis d'établir les bases nécessaires pour comprendre leur fonctionnement, en vue d'explorer leur application dans la conception d'un crypto-système chaotique à double retard utilisant des modulateurs Mach-Zehnder, sujet des prochains chapitres.

Chapitre II

Technique de Chiffrement Chaotique

II.1 Introduction

Dans un monde où la protection des informations est devenue une nécessité, la cryptographie joue un rôle essentiel en assurant la sécurité des communications et des données sensibles. Parmi les nombreuses approches développées, le chiffrement chaotique s'est imposé comme une alternative prometteuse, exploitant les propriétés des systèmes dynamiques chaotiques pour garantir un haut niveau de sécurité.

Ce chapitre explore les techniques de chiffrement chaotique. Nous commencerons par une présentation générale de la cryptographie, en distinguant les approches symétriques et asymétriques. Ensuite, nous approfondirons les différentes méthodes de chiffrement chaotique, notamment le chiffrement par addition, par modulation et par commutation. Enfin, nous aborderons les avancées dans le domaine des systèmes optiques chaotiques, qui ouvrent de nouvelles perspectives pour la sécurisation des communications.

L'objectif de ce chapitre est donc de fournir une compréhension approfondie des mécanismes de chiffrement chaotique.

II.2 Cryptographie

Le terme cryptographie provient des mots grecs qui signifient secret et écriture. Il englobe des techniques de cryptage des informations, permettant une communication sécurisée entre les parties Alice et Bob tout en empêchant l'adversaire Eve de comprendre, à l'aide d'une clé de cryptage. Une clé de déchiffrement est utilisée pour restaurer les informations sous une forme compréhensible. [16]

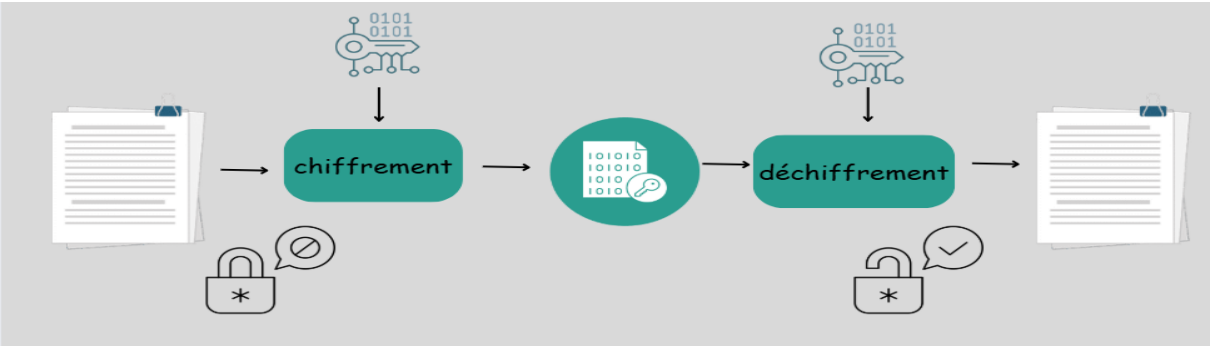

Figure II.1:le principe de chiffrement et déchiffrement

II.2.1 Cryptographie Symétrique

Le chiffrement symétrique implique l'utilisation de la même clé pour les processus de chiffrement et de déchiffrement. Plus précisément, Alice et Bob parviennent à un consensus clandestin sur une clé secrète K, qui est utilisée à la fois pour crypter et déchiffrer les messages. De plus, un algorithme cryptographique pour le chiffrement et le déchiffrement est également applicable. Ces systèmes bénéficient principalement de leur efficacité en termes de temps de calcul, applicable à la fois aux opérations de chiffrement et de déchiffrement. À l'inverse, la vulnérabilité de ce système provient de la nécessité d'une confidentialité absolue autour de la clé K. Historiquement, il s'agit du mode de paiement initial utilisé. De nombreux exemples de ce type existent, tels que le code de César et le bloc-notes à usage unique de Vernam . [17]

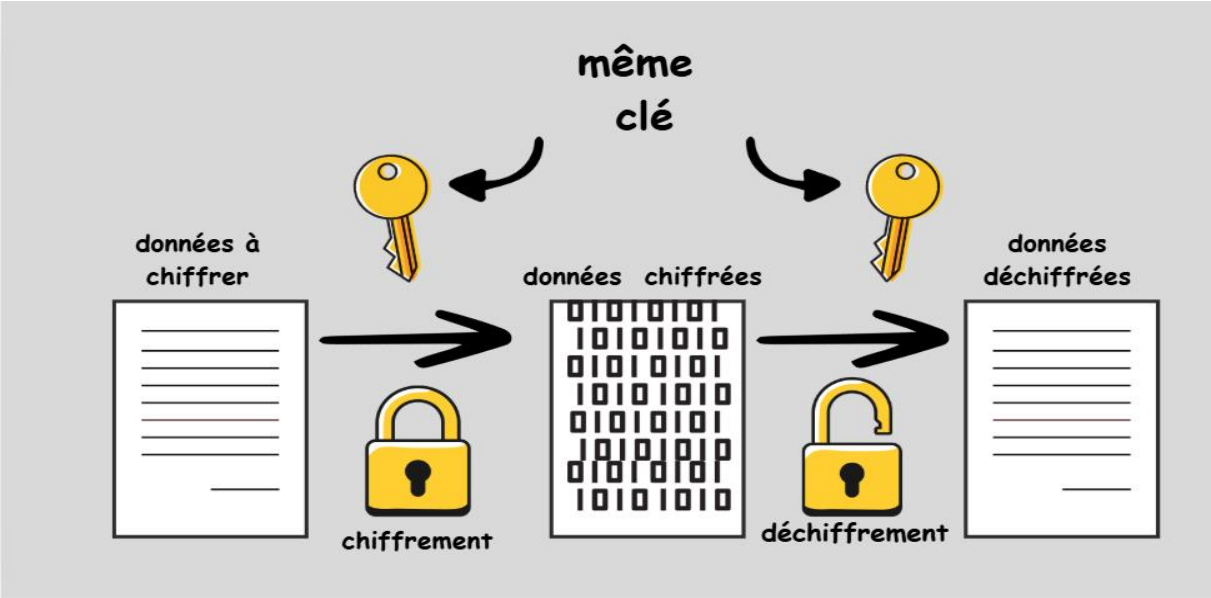

Figure II.2: Le principe de cryptographie symétrique

II.2.2 Cryptographie Asymétrique

Dans les systèmes symétriques, une clé unique est utilisée à la fois pour les processus d'écaillage et de déchirement. Le défi réside dans la transmission des clés : une clé distincte est requise pour chaque destinataire. À l'inverse, dans les systèmes asymétriques, chaque crypto-système est caractérisé par deux clés distinctes (une privée et une publique), ce qui rend extrêmement difficile de déduire la clé privée de la clé publique. Par conséquent, cela permet une distribution illimitée de la clé publique. [17]

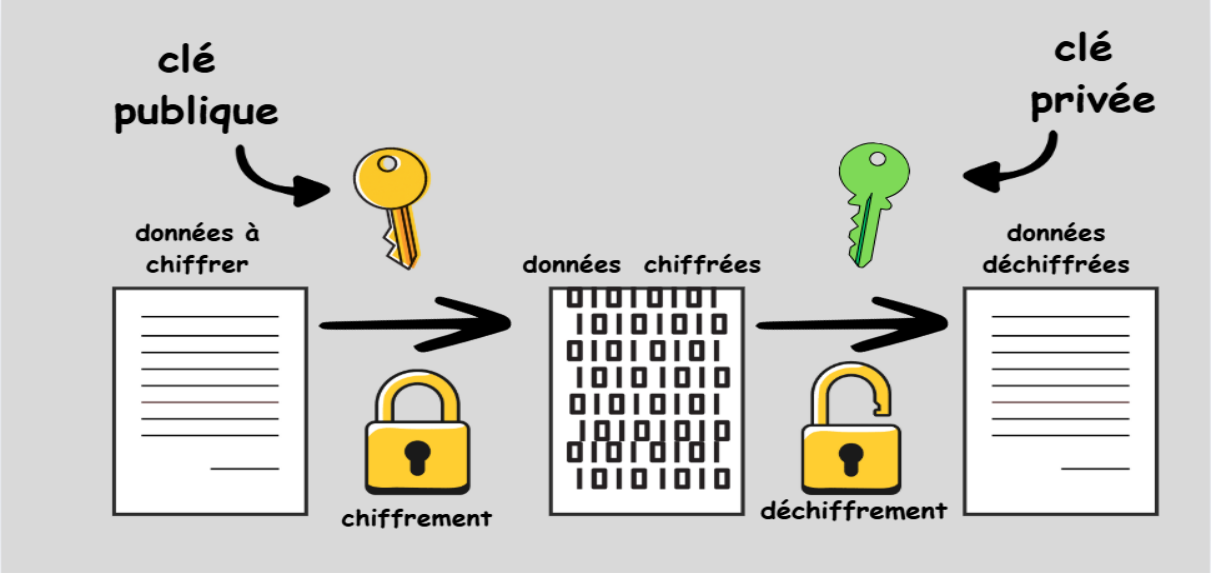

Figure II.3: Le principe de cryptographie asymétriques

II.3 Cryptographie chaotique

La cryptographie chaotique représente une approche sophistiquée de la sécurité de l'information, qui tire parti des caractéristiques des systèmes chaotiques, telles que leur sensibilité aux conditions initiales, leur imprévisibilité inhérente et leur nature déterministe non linéaire. Contrairement aux méthodes cryptographiques traditionnelles qui reposent sur des calculs arithmétiques ou algébriques, la cryptographie chaotique génère des signaux pseudo-aléatoires dérivés de systèmes dynamiques afin de faciliter les processus de chiffrement et de déchiffrement. En raison de leurs comportements complexes et de leur sensibilité aiguë aux paramètres initiaux, les systèmes chaotiques offrent un niveau de sécurité robuste tout en permettant des implémentations efficaces dans des applications de transmission sécurisées. [11]

- **Objectif principale**

L'objectif principale de la cryptographie chaotique est de

- Sécuriser la transmission d'informations en exploitant les dynamiques complexes des systèmes chaotiques.
- Rendre l'accès aux données impossible sans connaissance des paramètres du système chaotique (fonctions, conditions initiales…).

- Améliorer la performance des systèmes de communication, notamment dans les domaines optiques, sans fil ou haute fréquence.

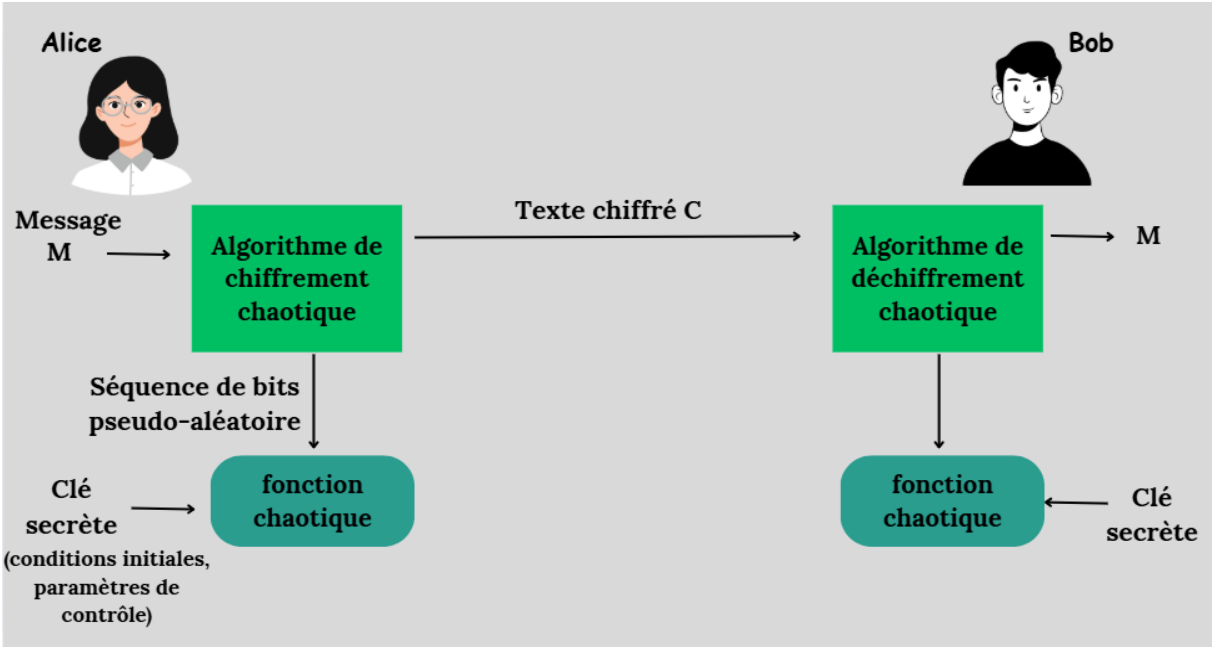

Figure II.4: Le principe d'un crypto-système chaotique

II.3.1 Chiffrement par Addition

Le masquage chaotique, ou chiffrement par addition, est une méthode de cryptage simple et efficace utilisée pour sécuriser la transmission des informations. Elle consiste à superposer le signal d'information *m(t)*, qu'il soit binaire ou analogique, à un signal chaotique porteur *x(t)* généré par l'émetteur. Cette combinaison permet de dissimuler le message dans un signal apparemment aléatoire, rendant son extraction difficile sans une synchronisation adéquate au niveau du récepteur. [18]

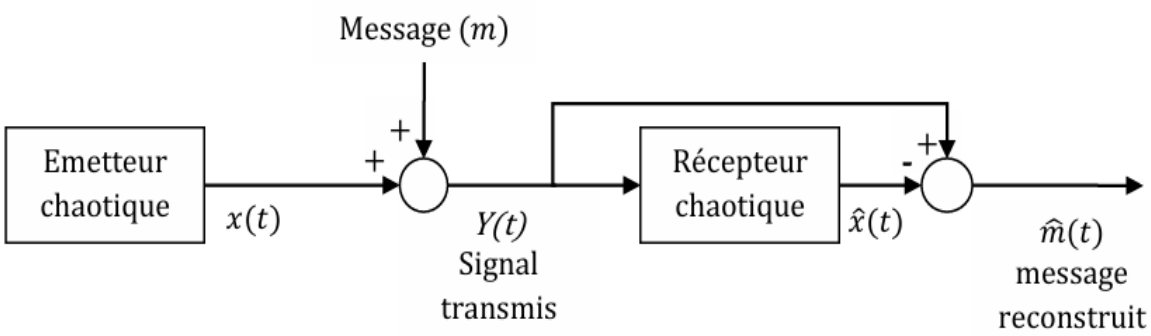

Figure II.5: Le Principe du cryptage par addition.[9]

Le principal avantage de cette méthode réside dans la simplicité du cryptage, ce qui permet son application aussi bien aux messages continus qu'aux messages discrets. Elle se révèle particulièrement efficace en l'absence de bruit dans le canal de transmission.

Cependant, pour assurer une synchronisation stable au niveau du récepteur et garantir la confidentialité de la transmission, la puissance du signal d'information doit être inférieure à celle du signal porteur, surtout en l'absence de bruit.

En revanche, lorsque le canal de transmission est bruité ou que l'émetteur chaotique présente des incertitudes paramétriques, les performances du système se dégradent significativement. Cela peut entraîner une perte de synchronisation entre l'émetteur et le récepteur (système maître et esclave), compromettant ainsi la transmission sécurisée des données. [18]

II.3.2 Chiffrement par Modulation

Cette méthodologie utilise un message qui encapsule des informations pour moduler un paramètre d'un émetteur chaotique. Un système de commande adaptatif est chargé d'assurer la synchronisation au niveau du récepteur tout en surveillant simultanément les modifications du paramètre modulé. Le schéma correspondant est illustré dans la figure II.6.

Au stade émetteur, la modulation d'un ou de plusieurs paramètres entraîne une modification persistante de la trajectoire vers divers attracteurs, ce qui produit un signal transmis plus sophistiqué qu'un signal chaotique standard. Néanmoins, la manière dont le message est intégré, et par conséquent le rôle de la modulation des paramètres, ne doivent pas compromettre les caractéristiques chaotiques du signal reçu. Il est essentiel de souligner que cette approche tire pleinement parti des avantages inhérents aux systèmes chaotiques et n'a pas d'équivalent dans les cadres de communication traditionnels. Il convient toutefois de noter que le chiffrement par modulation s'est révélé vulnérable à certaines formes d'attaques. [11]

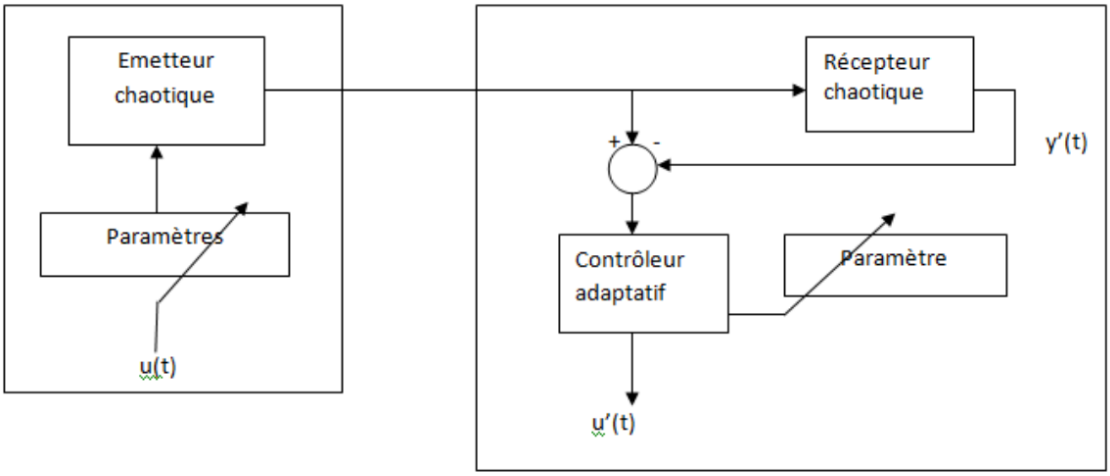

Figure II.6:Principe du chiffrement chaotique par modulation.[11]

II.3.3 Chiffrement par Commutation

Cette technique, impose que le message transmis soit de nature binaire. Son principe est illustré par le schéma de la figure.

L'émetteur chaotique est composé de deux oscillateurs générant respectivement les signaux chaotiques *x1(t)* et *x2(t)*. Le signal d'information binaire *m(t)* est utilisé pour commuter entre ces deux signaux :

- *x1(t)* encode le **bit 1**,
- *x2(t)* encode le **bit 0**.

Le signal résultant *x(t)* est ensuite transmis au récepteur via le canal de transmission.

Le récepteur est constitué de deux systèmes esclaves, chacun dédié à la synchronisation avec l'un des signaux chaotiques émis. Le premier système esclave est conçu pour se synchroniser exclusivement avec *x1(t) (*issu du premier oscillateur). La détection du bit 1 est confirmée lorsque l'erreur de synchronisation converge vers zéro, permettant ainsi la récupération du signal d'information à l'issue du processus de détection. [18]

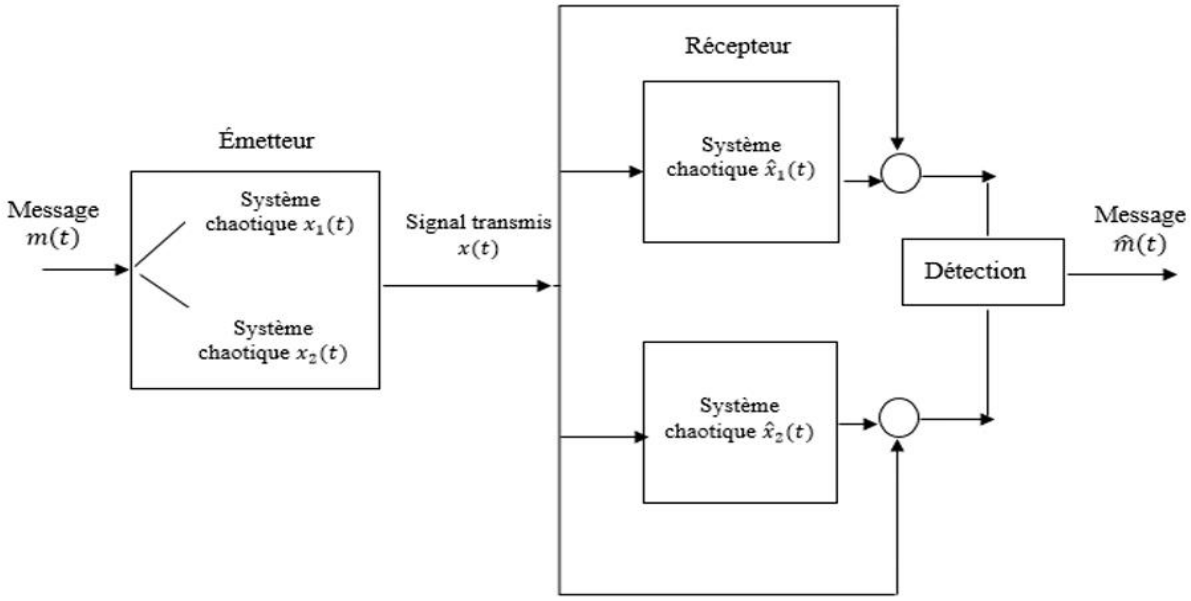

Figure II.7:Principe du cryptage par commutation.[11]

La commutation chaotique offre une meilleure robustesse au bruit de canal par rapport à la technique de masquage chaotique. Cependant, elle présente certaines limitations, notamment une vitesse de transmission réduite. En effet, à chaque changement de bit, un temps de convergence est nécessaire pour assurer la synchronisation, ce qui ralentit le processus de transmission.

De plus, cette technique souffre d'un faible niveau de sécurité. En raison des variations observables dans le signal chiffré à chaque changement du niveau binaire, un attaquant pourrait identifier des schémas exploitables, en particulier lorsque les deux oscillateurs utilisés dans l'émetteur possèdent des attracteurs très différents. Cette distinction entre les états du signal peut faciliter une tentative de déchiffrement ou d'interception non autorisée. [18]

II.4 Crypto-système optique chaotique

Les générateurs de chaos optiques exploitent la dynamique des oscillateurs à retard non linéaires, un concept exploré de manière significative par **Kensuke Ikeda** en 1979. Il a effectué des analyses numériques sur les fluctuations de puissance optique dans une cavité annulaire non linéaire connue sous le nom de boucle à retard, où un faisceau laser constant interagit avec lui-

même après la traversée de la cavité. La caractéristique unique des matériaux non linéaires, avec leurs indices de réfraction dépendant de l'intensité, entraîne des variations d'intensité lumineuse dues à des interférences, ce qui entraîne un comportement chaotique lorsque la lumière circule dans l'anneau. Les récents progrès en matière de communications chaotiques ont permis de transmettre avec succès des informations à des débits gigabits sur de grandes distances, en utilisant des signaux chaotiques générés par des systèmes entièrement optiques et électro-optiques. L'évolution de ces systèmes a donné naissance à trois catégories de crypto-systèmes optiques capables d'induire le chaos : les diodes laser à rétroaction, les modulateurs électro-optiques générant un chaos d'intensité et ceux produisant un chaos de phase. [11]

II.4.1 Systèmes à diode laser à rétroaction optique (chaos externe)

Ce type de système repose sur l'utilisation d'une diode laser à semi-conducteur dont l'émission est partiellement renvoyée vers elle-même par un miroir externe ou une fibre optique (rétroaction optique retardée). Ce rétrocontrôle induit des instabilités non linéaires dans le laser, pouvant conduire à un comportement chaotique.

Avantages :

- Haute bande passante du chaos (> GHz).
- Facilité d'intégration en composants photoniques.
- Synchronisation possible entre émetteur et récepteur pour des applications de chiffrement. [19]

II.4.2 Systèmes à modulateurs électro-optiques générant un chaos d'intensité

Ces systèmes utilisent des modulateurs électro-optiques (par exemple Mach-Zehnder ou Michelson) couplés à des boucles de rétroaction électroniques pour moduler l'intensité lumineuse d'un faisceau optique selon une loi non linéaire. La dynamique résultante peut présenter un comportement chaotique dans l'intensité du signal optique.

Avantages

- Architecture compacte et flexible.
- Bonne maîtrise du seuil de chaos (via la boucle électronique).
- Compatible avec l'intégration sur puce photonique. [20]

II.4.3 Systèmes à modulateurs générant un chaos de phase

Dans ce cas, les modulateurs électro-optiques sont utilisés pour induire des variations chaotiques dans la phase du signal optique plutôt que dans son intensité. Le chaos de phase est moins observable directement, ce qui en fait un outil intéressant pour le masquage sécurisé de l'information.

Avantages

- Plus grande discrétion du signal chaotique (le signal paraît stable en intensité).
- Meilleure résistance à l'interception non autorisée.
- Potentiel d'intégration dans les systèmes de transmission cohérente. [21]

II.5 Conclusion

Le chiffrement chaotique représente une approche innovante et prometteuse pour la sécurisation des communications, en exploitant les propriétés des systèmes dynamiques chaotiques. À travers ce chapitre, nous avons exploré les fondements de la cryptographie, distinguant les approches classiques symétriques et asymétriques avant d'analyser en détail les différentes techniques de chiffrement chaotique.

Les méthodes de chiffrement par addition, modulation et commutation offrent chacune des avantages spécifiques, mais elles présentent aussi certaines limites, notamment en termes de robustesse face aux interférences et aux attaques potentielles. Par ailleurs, l'essor des systèmes optiques chaotiques ouvre de nouvelles perspectives pour des applications à haut débit et à

longue distance, renforçant l'intérêt de ces technologies dans un contexte où la sécurité des données est primordiale.

Chapitre III

Evaluation des performances d'un crypto-système chaotique basé sur MZM

III.1 Introduction

Avec l'avènement des technologies de communication optique à haut débit, la protection de la transmission de l'information est devenue une préoccupation majeure. Les systèmes chaotiques, caractérisés par leur extrême sensibilité aux conditions initiales et leurs caractéristiques pseudo-aléatoires, présentent des opportunités prometteuses dans le domaine de la cryptographie, notamment grâce à l'utilisation de dispositifs optoélectroniques rapides et intégrables. Le modulateur électro-optique Mach-Zehnder (MZM) joue un rôle fondamental dans la génération de signaux chaotiques applicables au cryptage des données.

Ce chapitre vise à évaluer les caractéristiques de performance dynamiques, cryptographiques et pratiques d'un crypto-système optique chaotique qui utilise deux MZM. En utilisant des techniques analytiques qualitatives (attracteurs, bifurcations) et quantitatives (exposants de Lyapunov, dimension fractale), nous étudierons la complexité du signal généré et son efficacité en matière de transmission sécurisée. À terme, les simulations faciliteront l'évaluation de la résilience du système dans des conditions bruyantes, déterminant ainsi sa fiabilité dans des environnements pratiques.

III.2 Présentation du Modulateur Mach-Zehnder

Le modulateur Mach-Zehnder constitue un appareil électro-optique utilisé pour moduler l'amplitude d'une onde lumineuse. Ce dispositif fonctionne selon les principes d'une architecture d'interféromètre comportant des guides d'ondes intégrés, dans laquelle le faisceau lumineux incident est bifurqué en deux voies distinctes. Lors de l'application d'une tension électrique à l'une des voies, une modification de l'indice de réfraction se produit en raison de l'effet électro-optique, induisant ainsi un déphasage de l'onde optique traversant cette voie.

Ensuite, les deux ondes optiques sont recombinées en sortie. La disparité de phase qui en résulte entre ces ondes engendre un phénomène d'interférence constructive ou destructive, aboutissant à la modulation de l'intensité du signal optique en sortie. Ce principe fondamental facilite le contrôle précis de la transmission ou de l'atténuation du signal lumineux, avec une précision exceptionnelle et à des fréquences extrêmement élevées, ce qui en fait un élément essentiel des systèmes de communication optique et de cryptographie chaotique. [22]

Le fonctionnement d'un modulateur Mach-Zehnder repose sur l'interférence entre deux ondes optiques ayant parcouru deux bras distincts. Lorsqu'une tension V est appliquée sur l'un des bras, elle induit un décalage de phaseΔ_{φ}par effet électro-optique. L'intensité du signal optique en sortie dépend directement de ce déphasage :

$$\Delta_{\varphi} = \pi \frac{V}{V_{\pi}}$$

- Δ_{φ}est le déphasage entre les deux bras.
- Vest la tension appliquée.
- V_{π}est la tension pour laquelle un déphasage de π est obtenu (tension de demi-onde).

L'intensité normalisée du signal en sortie est donnée par :

$$I_{out} = I_0 cos^2(\frac{\Delta_{\varphi}}{2})$$

$$\rightarrow \frac{I_{out}}{I_0} = cos^2(\frac{\pi V}{2V_{\pi}})$$

- I_0est l'intensité du signal optique incident

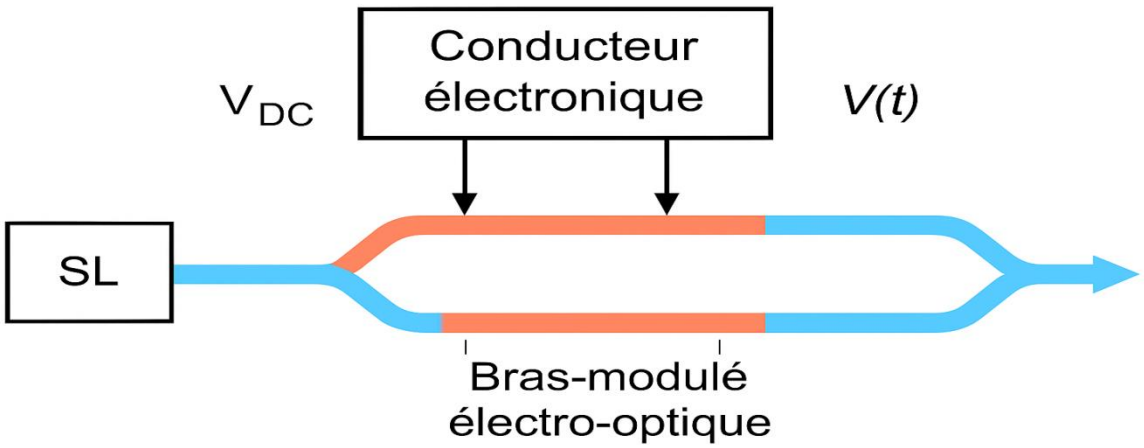

Figure III.1:Principe de fonctionnement du modulateur Mach Zehnder

Il est important de noter que la tension de demi-ondeV_{π}, définie comme la tension nécessaire pour induire un déphasage de πentre les deux bras de l'interféromètre, varie en fonction du régime d'utilisation du modulateur.

En pratique, on distingue deux valeurs :

- $V_{\pi DC}$: la tension de demi-onde mesurée en régime statique (ou basse fréquence), utilisée pour les tests ou la modulation lente.
- $V_{\pi RF}$: la tension de demi-onde en régime dynamique (à haute fréquence, typiquement GHz), utilisée dans les applications réelles de transmission optique.

La valeur de$V_{\pi RF}$est généralement plus élevée que$V_{\pi DC}$en raison des pertes et limitations des composants à haute fréquence (effets capacitifs, résistifs, dispersion, etc.).

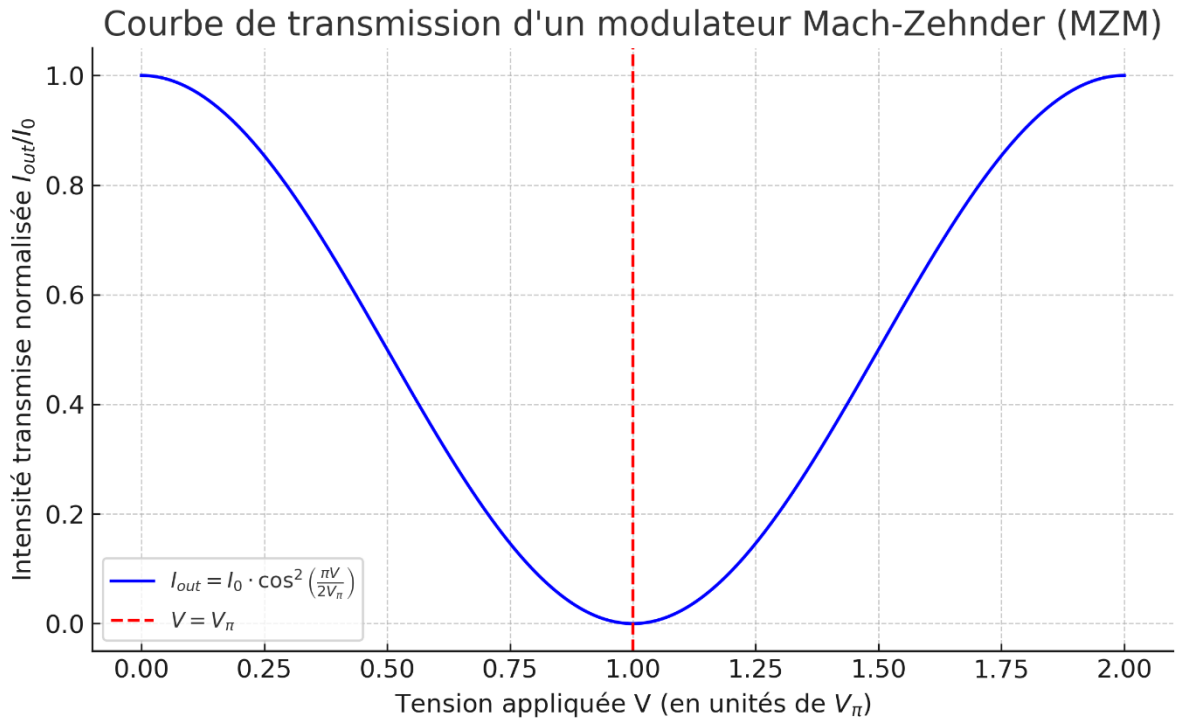

Figure III.2:Courbe de transmission d'un modulateur Mach Zehnder

- ✓ Si $V = 0 \Rightarrow \Delta_\varphi = 0 \Rightarrow$**transmission maximale**.
- ✓ Si $V = V_\pi \Rightarrow \Delta_\varphi = \pi \Rightarrow$**transmission nulle (extinction).**

La variation de$V$permet donc de moduler l'intensité de façon continue ou binaire (ON/OFF).

III.3 Architecture du Système Chaotique à base de deux MZM à rétroaction

Nous nous proposons ici d'examiner et de mesurer les capacités fonctionnelles du crypto-système décrit par les figures III.3 et III.4.

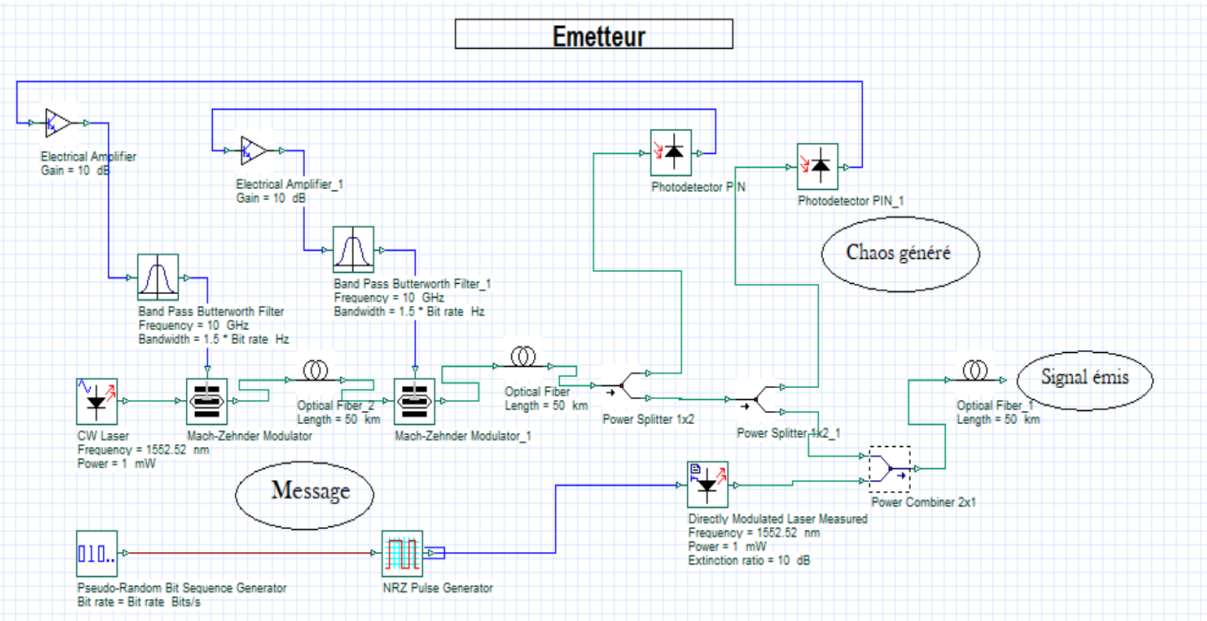

Figure III.3:Émetteur du système de chiffrement chaotique à double MZM avec rétroaction

Nous avons au niveau d'émetteur :

- Un module dédié à la génération du signal chaotique optique.
- Un module pour générer et moduler le message.
- Un module de chiffrement chaotique basé sur une combinaison optique.

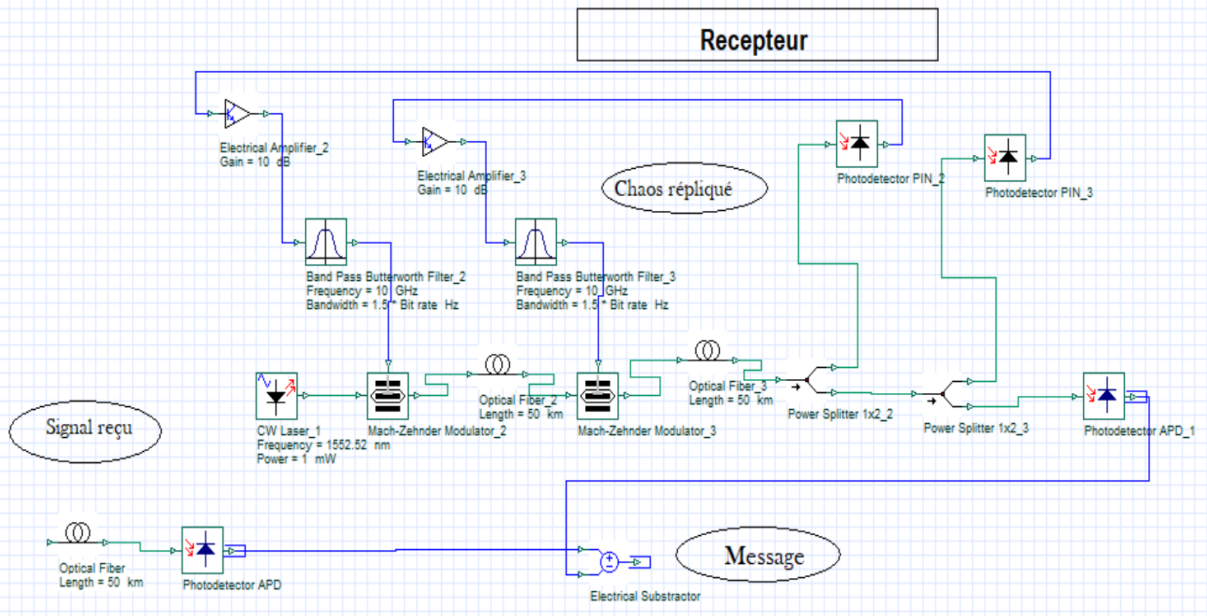

Figure III.4:Récepteur du système de chiffrement chaotique à double MZM avec rétroaction.

Au niveau du récepteur :

- Un module de synchronisation du signal optique.
- Un module dédié à la génération du signal chaotique optique.
- Un module dédié au déchiffrement du message optique.

III.3.1 Modélisation du système

- Un laser à semi-conducteur fonctionnant en régime continu (CW) émet une puissance lumineuse constante donnée par l'expression

$$P = hvN$$

Où :

  - h est la constante de Planck.
  - v est la fréquence d'émission des photons.
  - N est le nombre de photons émis par seconde.

- Deux modulateurs Mach-Zehnder

La lumière issue de la source laser est répartie de manière égale entre les deux bras du modulateur Mach-Zehnder (MZM**)**. À la sortie du dispositif, les deux faisceaux interfèrent, produisant une modulation en fonction de la différence de phase accumulée dans chaque bras.

L'indice de réfraction dans l'un des bras est modulé par une tension électrique issue d'un circuit de commande. Cette tension appliquée comporte généralement deux composantes :

- Une composante continueV_{DC_i}, utilisée pour fixer le point de fonctionnement optimal du modulateur.
- Une composante radiofréquenceV_{RF_i}, qui peut provenir d'un circuit chaotique et est destinée à générer une modulation dynamique du champ optique, condition nécessaire à l'apparition du chaos optique dans certains systèmes.

Le champ électrique complexe en sortie du MZM peut être formulé par l'équation suivante :

$$E_i(t) = \frac{1}{2}E_0\left\{1 + e^{\left(\frac{\pi V_i(t)}{V_{\pi RF_i}} + \frac{\pi V_{DC_i}}{V_{\pi DC_i}}\right)}\right\}$$

La puissance de sortie optique du modulateur 1 est

$$P_1(t) = P_0 cos^2\left[\frac{\pi V_1(t)}{V_{\pi RF_1}} + \frac{\pi V_{DC_1}}{2V_{\pi DC_1}}\right]$$

Où : $P_0 = {E_0}^2$

La puissance de sortie optique du modulateur 2 est

$$P_2(t) = P_1 cos^2\left[\frac{\pi V_2(t)}{V_{\pi RF_2}} + \frac{\pi V_{DC_2}}{2V_{\pi DC_2}}\right]$$

- Deux photodiodes de sensibilités S_1 et S_2 permet de convertir l'intensité lumineuse incidente en un signal électrique mesurable.
- Deux amplificateurs de gains G_1 et G_2.
- Deux lignes à retard optique en fibre : sont utilisées pour introduire des décalages temporels T_1 et T_2 dans le signal optique. La fibre est considérée comme non dispersive, c'est-à-dire que le retard est indépendant de la fréquence du signal. Dans ce cas, le retard temporel T total s'exprime par la relation suivante :

$$T = T_1 + T_2 = \frac{L_1}{V_g} + \frac{L_2}{V_g}$$

Où :

  - L_1 et L_2 sont les longueurs de la fibre correspondants aux deux retards.
  - V_g est la vitesse de groupe de la propagation dans la fibre.

- Deux filtres RF passe-bande [F_{11},F_{12}] et [F_{21},F_{22}] respectivement.

$$H_F(p) = \frac{\tau_2 p}{(1 + \tau_2 p)(1 + \tau_1 p)}$$

Où : $\tau_{i1} = \frac{1}{2\pi F_{i1}}$ et $\tau_{i2} = \frac{1}{2\pi F_{i2}}$ $;i = 1,2$

Filtre	Type de représentation dans le domaine temporel	Bande passante
Passe-bas de 1er ordre	$x(t) + \tau \frac{dx(t)}{dt}$	$[0, f_H = \frac{1}{2\pi\tau}]$
Passe-bande de 1er ordre	$\left(1 + \frac{\tau_1}{\tau_2}\right) x(t) + \tau_1 \frac{dx(t)}{dt} + \frac{1}{\tau_2} \int_{t_0}^{t} x(t')dt'$	$[f_B, f_H]$
Passe-haut 1er ordre	$x(t) + \frac{1}{\tau} \int_{t_0}^{t} x(t')dt'$	$[f_B = \frac{1}{2\pi\tau'} \infty]$

Tableau III.1:Filtres et leurs équations correspondantes.[8]

Par conséquent, le système est représenté par un ensemble de deux équations, permettant notamment de déterminer la tension RF en sortie

Equation 1

$$\left(1 + \frac{\tau_{11}}{\tau_{12}}\right) \dot{V}_1(t) + \tau_{11} \ddot{V}_1(t) + \frac{1}{\tau_{12}} V_1(t) = G_1 S_1 \dot{P}_2(t - T)$$

$$\left(1 + \frac{\tau_{11}}{\tau_{12}}\right) \dot{V}_1(t) + \tau_{11} \ddot{V}_1(t) + \frac{1}{\tau_{12}} V_1(t)$$
$$= -\frac{\pi}{2} \frac{G_1 S_1 P_0}{V_{\pi RF_1}} \dot{V}_1(t - T) sin\left[\frac{\pi V_1(t - T)}{V_{\pi RF_1}} + \frac{\pi V_{DC_1}}{V_{\pi DC_1}}\right] cos^2\left[\frac{\pi V_2(t - T)}{2V_{\pi RF_2}} + \frac{\pi V_{DC_2}}{2V_{\pi DC_2}}\right]$$
$$- \frac{\pi}{2} \frac{G_1 S_1 P_0}{V_{\pi RF_2}} \dot{V}_2(t - T) sin\left[\frac{\pi V_2(t - T)}{V_{\pi RF_2}} + \frac{\pi V_{DC_2}}{V_{\pi DC_2}}\right] cos^2\left[\frac{\pi V_1(t - T)}{2V_{\pi RF_1}} + \frac{\pi V_{DC_1}}{2V_{\pi DC_1}}\right]$$

Posons

$\frac{\pi}{2} \frac{G_1 S_1 P_0}{V_{\pi RF_1}} = \beta_{11}$, $\frac{\pi}{2} \frac{G_1 S_1 P_0}{V_{\pi RF_2}} = \beta_{12}$, $\frac{\pi V_{DC_1}}{V_{\pi DC_1}} = \varphi_1$, $\frac{\pi V_{DC_2}}{V_{\pi DC_2}} = \varphi_2$

Il s'en suit

$$\left(1+\frac{\tau_{11}}{\tau_{12}}\right)\dot{V}_1(t)+\tau_{11}\ddot{V}_1(t)+\frac{1}{\tau_{12}}V_1(t) + \beta_{11}\dot{V}_1(t-T)sin\left[\frac{\pi V_1(t-T)}{V_{\pi RF_1}}+\varphi_1\right]cos^2\left[\frac{\pi V_2(t-T)}{V_{\pi RF_2}}+\frac{\varphi_2}{2}\right] + \beta_{12}\dot{V}_2(t-T)sin\left[\frac{\pi V_2(t-T)}{V_{\pi RF_2}}+\varphi_2\right]cos^2\left[\frac{\pi V_1(t-T)}{V_{\pi RF_1}}+\frac{\varphi_1}{2}\right]=0$$

Equation 2

$$\left(1+\frac{\tau_{21}}{\tau_{22}}\right)\dot{V}_2(t)+\tau_{21}\ddot{V}_2(t)+\frac{1}{\tau_{22}}V_2(t)=G_2S_2\dot{P}_2(t-T)$$

En posant à nouveau

$\beta_{21}=\frac{\pi}{2}\frac{G_2S_2P_0}{V_{\pi RF_1}}$; $\beta_{22}=\frac{\pi}{2}\frac{G_2S_2P_0}{V_{\pi RF_2}}$

On obtient

$$\left(1+\frac{\tau_{21}}{\tau_{22}}\right)\dot{V}_2(t)+\tau_{21}\ddot{V}_2(t)+\frac{1}{\tau_{22}}V_2(t) + \beta_{21}\dot{V}_1(t-T)sin\left[\frac{\pi V_1(t-T)}{V_{\pi RF_1}}+\varphi_1\right]cos^2\left[\frac{\pi V_2(t-T)}{V_{\pi RF_2}}+\frac{\varphi_2}{2}\right] + \beta_{22}\dot{V}_2(t-T)sin\left[\frac{\pi V_2(t-T)}{V_{\pi RF_2}}+\varphi_2\right]cos^2\left[\frac{\pi V_1(t-T)}{V_{\pi RF_1}}+\frac{\varphi_1}{2}\right]=0$$

III.3.2 Constantes et coefficients du modèle

Le système se caractérise par les paramètres suivants

τ_{11} ,τ_{12} , τ_{21} , τ_{22} , β_{11} , β_{12} , β_{21} , β_{22} , T , $V_{\pi RF1}$, $V_{\pi RF2}$, φ_1 et φ_2.

Dans le cadre de cette étude, les constantes suivantes ont été fixéesτ_{11} , τ_{12} , τ_{21} , τ_{22} , T , $V_{\pi RF1}$, $V_{\pi RF2}$, φ_1 et φ_2, et nous avons caractérisé l'évolution du système selon les variations deβ_{11} , β_{12} , β_{21}, β_{22}.

Les paramètres mentionnés sont regroupés dans le tableau III.2

$\tau_{11}(\mu s)$	$\tau_{12}(\mu s)$	$\tau_{21}(ns)$	$\tau_{22}(ns)$	$\mathrm{T}(ns)$	$V_{\pi RF1(V)}$	$V_{\pi RF2(V)}$	$\varphi_{1(rad)}$	$\varphi_{2(rad)}$
$\frac{1}{2\pi}$	$\frac{1}{2\pi}$	$\frac{1}{2\pi}$	$\frac{1}{2\pi}$	10	5	5	$\frac{\pi}{4}$	$\frac{\pi}{4}$

Tableau III.2:les valeurs du modèle utilisée

Pour garantir la sécurité du crypto-système, les valeurs de ces paramètres doivent être choisies de manière non triviale et conservées confidentielles, car elles en constituent la clé cryptographique.

III.4 Étude Comportementale du Système par Simulation

III.4.1 Méthodes numériques pour la résolution des équations

Les techniques numériques permettant de résoudre les équations différentielles se répartissent généralement en deux grandes familles : les méthodes explicites et les méthodes implicites.

Une méthode explicite calcule directement la valeur à venir à partir des valeurs déjà connues, tandis qu'une méthode implicite définit la valeur future via une équation qui la relie implicitement à elle-même ou à d'autres inconnues.

Pour résoudre une équation différentielle ordinaire (EDO), il est habituel de disposer des conditions initiales — une étape fondamentale appelée « problème aux valeurs initiales » ou « problème de Cauchy ». Par exemple, pour une EDO d'ordre deux, la connaissance des valeurs initiales y(0) et y′(0) suffit à déterminer la solution.

Cependant, lorsqu'on traite des équations différentielles à retard (EDR), la situation devient plus complexe. En effet, la présence d'un retard temporel T nécessite de connaître la fonction solution sur un intervalle temporel, typiquement [0,T], avant même de commencer le calcul. Cette exigence signifie que la condition initiale n'est plus un simple point, mais une fonction définie sur un intervalle, représentant une infinité de données initiales.

Cette caractéristique rend l'étude des EDR particulièrement intéressante dans le cadre de la cryptographie chaotique, car certaines solutions exhibent un comportement chaotique

complexe. Ces solutions ne peuvent être entièrement prédéterminées uniquement à partir de la modélisation mathématique du système, ce qui contribue à renforcer la sécurité du système cryptographique.

Dans ce contexte, nous présenterons deux méthodes d'intégration numérique fréquemment utilisées : la méthode d'Euler et la méthode de Runge-Kutta, qui seront détaillées dans les sections suivantes. [11]

− Méthode d'Euler

Dans les systèmes de chiffrement basés sur le chaos, la méthode d'Euler constitue un outil fondamental pour la discrétisation des équations différentielles ordinaires qui modélisent les comportements dynamiques. Elle permet de transformer un système chaotique continu, tel que celui de Lorenz ou de Rossler, en une version discrète exploitable dans des simulations numériques. Le calcul se fait de manière itérative à l'aide de la formule $x_{n+1} = x_n + h \cdot f(x_n, t_n)$, avec h représentant le pas de temps. Cette méthode, bien que simple et rapide à mettre en œuvre, requiert un choix judicieux du pas pour éviter une dégradation de la précision, ce qui pourrait nuireà la complexité du signal chaotique produit, et donc à la sécurité du chiffrement. [23]

− Méthode de Runge-Kutta d'ordre 4

La méthode de Runge-Kutta d'ordre 4 (RK4) constitue une approche numérique très utilisée pour la résolution des équations différentielles ordinaires, notamment dans les systèmes dynamiques. Elle se distingue par son équilibre entre simplicité d'implémentation et précision, en effectuant quatre calculs intermédiaires de la dérivée au sein de chaque intervalle de temps. Cette stratégie permet d'obtenir une estimation plus fiable de la solution comparée aux méthodes plus simples comme celle d'Euler. RK4 se révèle particulièrement efficace pour les simulations nécessitant une grande stabilité, comme celles impliquant des modèles mécaniques issus de la formulation de Lagrange. Grâce à sa capacité à offrir des résultats cohérents même sur de longues périodes de calcul, elle demeure une solution de référence dans les environnements de simulation numérique. [24]

III.4.2 Implémentation sous Matlab

La résolution a été effectuée à l'aide de la fonction DDE23, basée sur une méthode de type Runge-Kutta adaptée aux équations différentielles à retard.

A partir des 2 équations du 2^{éme} ordre, on obtient un système à 4 équations du 1er ordre

On pose :

- $V_1(t) = y_2(t)$, $\dot{V}_1(t) = y_1(t)$

  [où : $\ddot{V}_1(t) = \dot{y}_2(t)$]

- $V_2(t) = y_4(t)$, $\dot{V}_2(t) = y_3(t)$

  [où : $\ddot{V}_2(t) = \dot{y}_3(t)$]

$$\dot{y}_1(t) = -\left[\left(\frac{1}{\tau_{11}} + \frac{1}{\tau_{12}}\right) y_1(t) + \frac{1}{\tau_{11}\tau_{12}} y_2(t)\right] - \frac{\beta_{11}}{\tau_{11}} y_1(t-T) \sin\left[\frac{\pi y_2(t-T)}{V_{\pi RF_1}} + \varphi_1\right] cos^2\left[\frac{\pi y_4(t-T)}{V_{\pi RF_2}} + \frac{\varphi_2}{2}\right] - \frac{\beta_{12}}{\tau_{11}} y_3(t-T) \sin[\frac{\pi y_4(t-T)}{V_{\pi RF_2}} + \varphi_2] cos^2[\frac{\pi y_2(t-T)}{V_{\pi RF_1}} + \frac{\varphi_1}{2}]$$

$$\dot{y}_2(t) = y_1(t)$$

$$\dot{y}_3(t) = -\left[\left(\frac{1}{\tau_{21}} + \frac{1}{\tau_{22}}\right) y_3(t) + \frac{1}{\tau_{21}\tau_{22}} y_4(t)\right] - \frac{\beta_{21}}{\tau_{21}} y_1(t-T) \sin\left[\frac{\pi y_2(t-T)}{V_{\pi RF_1}} + \varphi_1\right] cos^2\left[\frac{\pi y_4(t-T)}{V_{\pi RF_2}} + \frac{\varphi_2}{2}\right] - \frac{\beta_{22}}{\tau_{21}} y_3(t-T) \sin[\frac{\pi y_4(t-T)}{V_{\pi RF_2}} + \varphi_2] cos^2[\frac{\pi y_2(t-T)}{V_{\pi RF_1}} + \frac{\varphi_1}{2}]$$

$$\dot{y}_4(t) = y_3(t)$$

III.4.3 Caractérisation du chaos

Ce travail nous a permis de déterminer les caractéristiques suivantes.

III.4.3.1 Le diagramme de bifurcation

Le script Matlab employé pour la génération du diagramme de bifurcation est le suivant :

```
%Diagramme de bifurcation
bmin=0.0001;
bmax=1;
bint=0.0001;

brange=[bmin bint bmax];
bifurcation2(brange);
function D = bifurcation2(range)

%
 D=[];

  for b=range(1):range(2):range(3)
     fprintf('b=%g...\n',b);

     % on fait varier b11 et b12, les autres restent constants

 b21=0.009;
 b22=0.008;


        solb = dde23(@chaosff,10*10^-9,[10^-3;0;10^-3;0],[0,2*10^-7],[],b,b,b21,b22);

     for i=2:length(solb.y(2,:))-1
        if((solb.y(2,i)>solb.y(2,i-1))&&(solb.y(2,i)>solb.y(2,i+1)))
            D=[D; b solb.y(2,i)];
         end
     end
 end
 figure(3)
  plot(D(:,1),D(:,2),'ro','MarkerEdgeColor','b','MarkerFaceColor','b','MarkerSize',1.5)
```

III.4.3.2 L'évolution temporelle du signal chaotique

Le script Matlab permettant de réaliser l'intégration numérique ainsi que la représentation temporelle du signal est présentée ci-dessous :

```
function sol = chaos
%
 T=3e-6;
 b11=0.009;
 b12=0.008;
 b21=0.009;
 b22=0.008;

sol = dde23(@chaosff,10*10^-9,[10^-6;-1;10^-6;-1],[0,T],[],b11,b12,b21,b22);
% Représentation temporelle
figure(1)
plot(sol.x,sol.y(2,:));
% ------------------------------------------------------------------------------------------------------------
function yp = chaosff(t,y,Z,b11,b12,b21,b22)
%
to11 =1/(2*pi*10^9);
to12 = 1/(2*pi*10^6);
to21 = to11+0.2;
to22 = to12+0.2;
%
Vprf1 = 5.0;
Vprf2 = 5.0;
%
phi1 = pi/4;
phi2 = pi/4;
%
ylag1= Z(:,1);

yp = zeros(4,1);
%
yp(2) = -((1/to11)+(1/to12))*y(2)-(1/to11*to12)*y(1)-(b11/to11)*ylag1(2)*(sin((pi*ylag1(1))/Vprf1+phi1))*
yp(1) = y(2);
%
yp(4) = -((1/to21)+(1/to22))*y(4)-(1/to21*to22)*y(3)-(b21/to21)*ylag1(2)*(sin((pi*ylag1(1))/Vprf1+phi1))*
yp(3) = y(4);
```

Voici la suite du programme yp(2) et yp(4) respectivement :

```
(cos((pi*ylag1(3))/Vprf2+(phi2/2)))^2-(b12/to11)*ylag1(4)*(sin((pi*ylag1(3))/Vprf2+phi2))*(cos((pi*ylag1(1))/Vprf1+phi1/2))^2;
```

```
(cos((pi*ylag1(3))/Vprf2+(phi2/2)))^2-(b22/to21)*ylag1(4)*(sin((pi*ylag1(3))/Vprf2+phi2))*(cos((pi*ylag1(1))/Vprf1+phi1/2))^2;
```

III.4.3.3 La densité spectrale de puissance

Le script Matlab permettant de calculer la densité spectrale de puissance est présenté ci-dessous :

```
%spectre
Te=0.01e-9;

Fe=1/Te;
N=round((T/Te)/2);

t = linspace (T/2,T,N);
y = deval(sol,t);
f=0:Fe/N:Fe/2-Fe/N;
figure(10)
dsp=(abs(fft(y(2,:)))).^2);
plot(f,10*log(dsp(1:length(f))+0.0000000001))
```

III.4.3.4 Le plan de phase

Le script Matlab utilisé pour visualiser l'espace des phases et le plan de phase est le suivant :

```
%Espace de phase 3D
figure(6)
tau=0.3*10^-6;
t = linspace(2*tau,T,10000);
y = deval(sol, t)/0.5e-6;
yy = deval(sol, t - tau)/0.5e-6;
yyy = deval(sol,t - 2*tau)/0.5e-6;
plot3(y(2,:),yy(2,:),yyy(2,:),'.')
 %plan de phase
 figure(12)
 plot(y(2,:),yy(2,:),'.')
```

III.4.4 Chiffrement-déchiffrement

Les opérations de chiffrement et de déchiffrement ont été effectuées à l'aide de la plateforme OptiSystem. En l'absence de possibilité de générer un réplica synchronisé du signal chaotique à la réception directement sous MATLAB, une approche alternative a été adoptée : le signal chaotique à l'émission a été généré sous MATLAB via une intégration numérique, puis enregistré dans un fichier au format .dat. Ce fichier a ensuite été importé dans OptiSystem afin de réaliser les étapes de chiffrement et de déchiffrement, conformément au schéma présenté dans la figure III.6

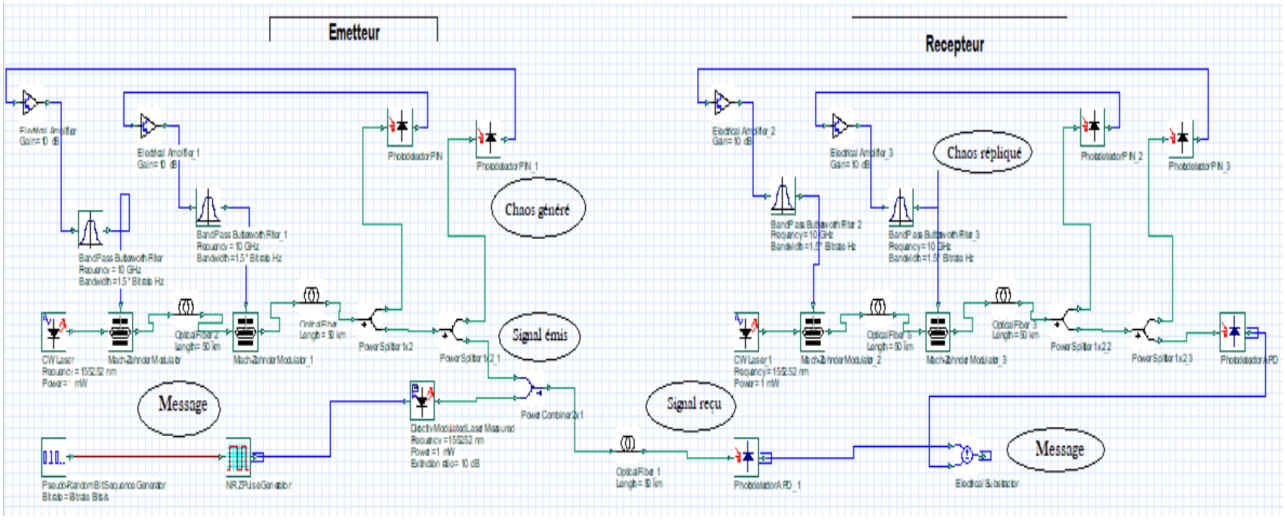

Figure III.5:Schéma du chiffrement-déchiffrement

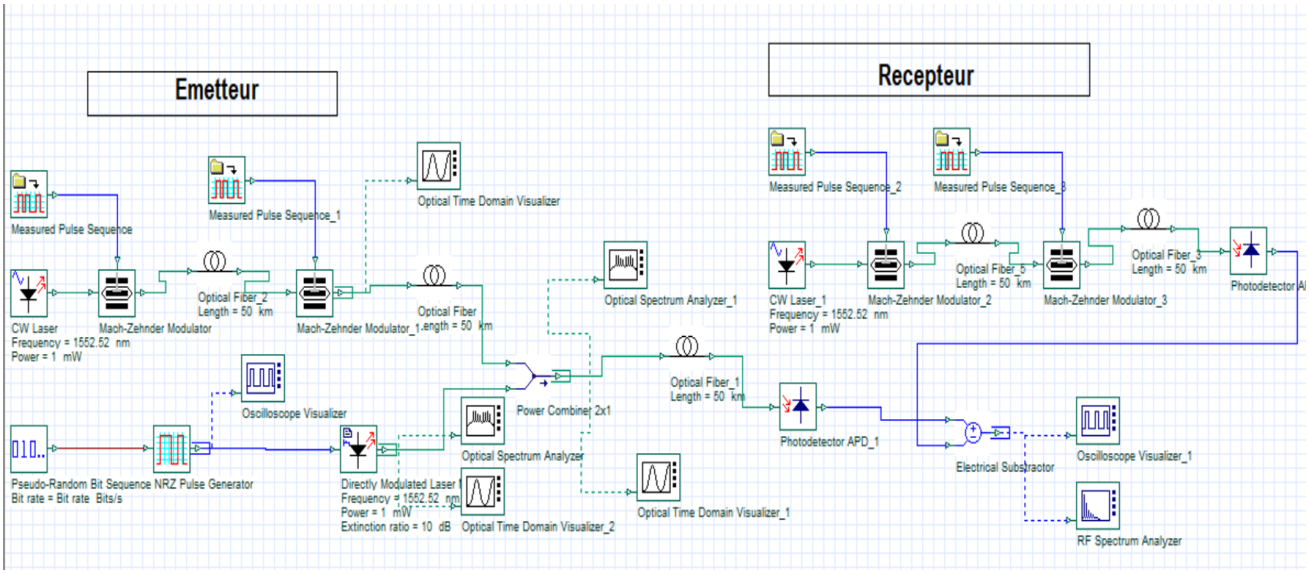

Figure III.6:Schéma du chiffrement-déchiffrement adaptée

III.5 Résultats de simulation

1. Le diagramme de bifurcation

L'évolution du comportement dynamique du système en fonction de β_{11} et β_{12} est représentée sous forme de diagramme de bifurcation dans la figure III.7

Il apparaît que le système entre en régime chaotique dès que $\beta_{11} = 0.23$ et $\beta_{12} = 0.23$. De plus, une augmentation des valeurs de β intensifie nettement le caractère chaotique du système.

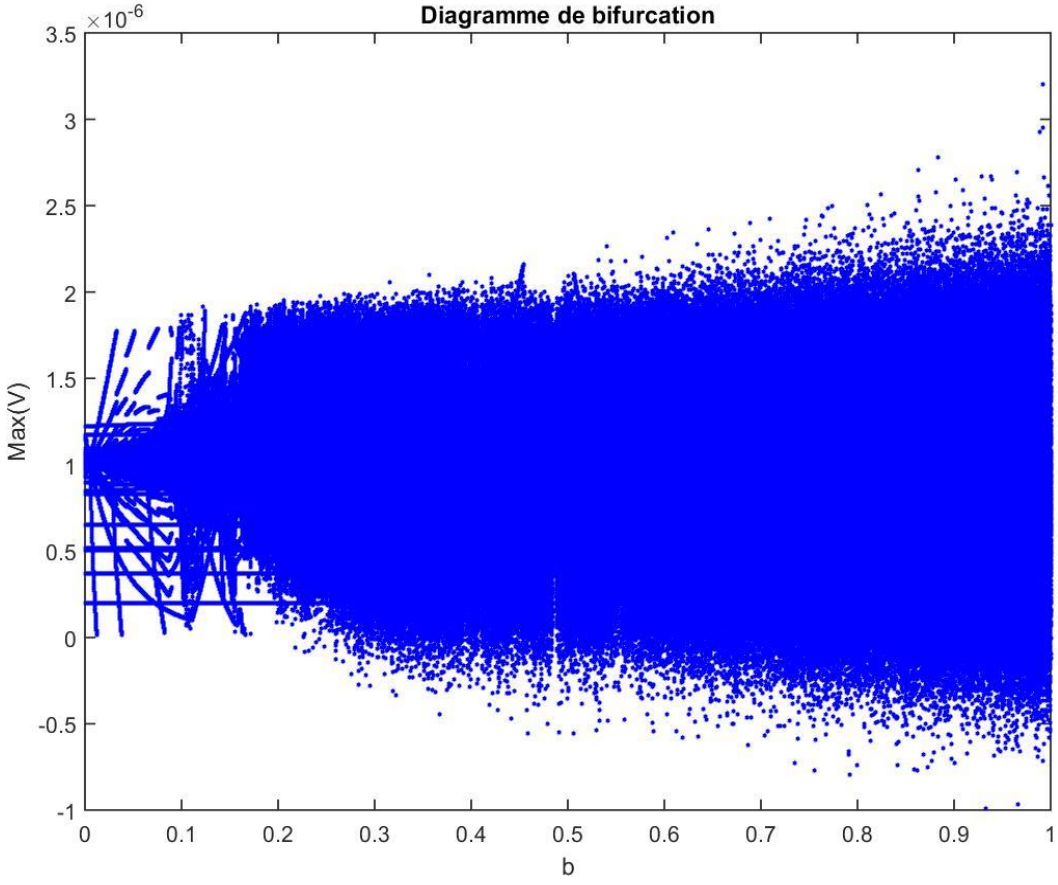

Figure III.7:Diagramme de bifurcation en fonction des paramètres de contrôle beta.

2. Etude pour $\boldsymbol{\beta_{11} = \beta_{21} = 0.009}$ et $\boldsymbol{\beta_{12} = \beta_{22} = 0.008}$

La représentation temporelle du signal *v(t)*, en sortie du filtre passe-bande, révèle un comportement périodique du système. figure III.8 et figure III.9

L'analyse fréquentielle met en évidence une fréquence fondamentale unique, accompagnée de plusieurs harmoniques. Figure III.10

Un attracteur cyclique (cycle limite) est clairement visible dans le plan de phase, confirmant un comportement périodique. Figure III.11

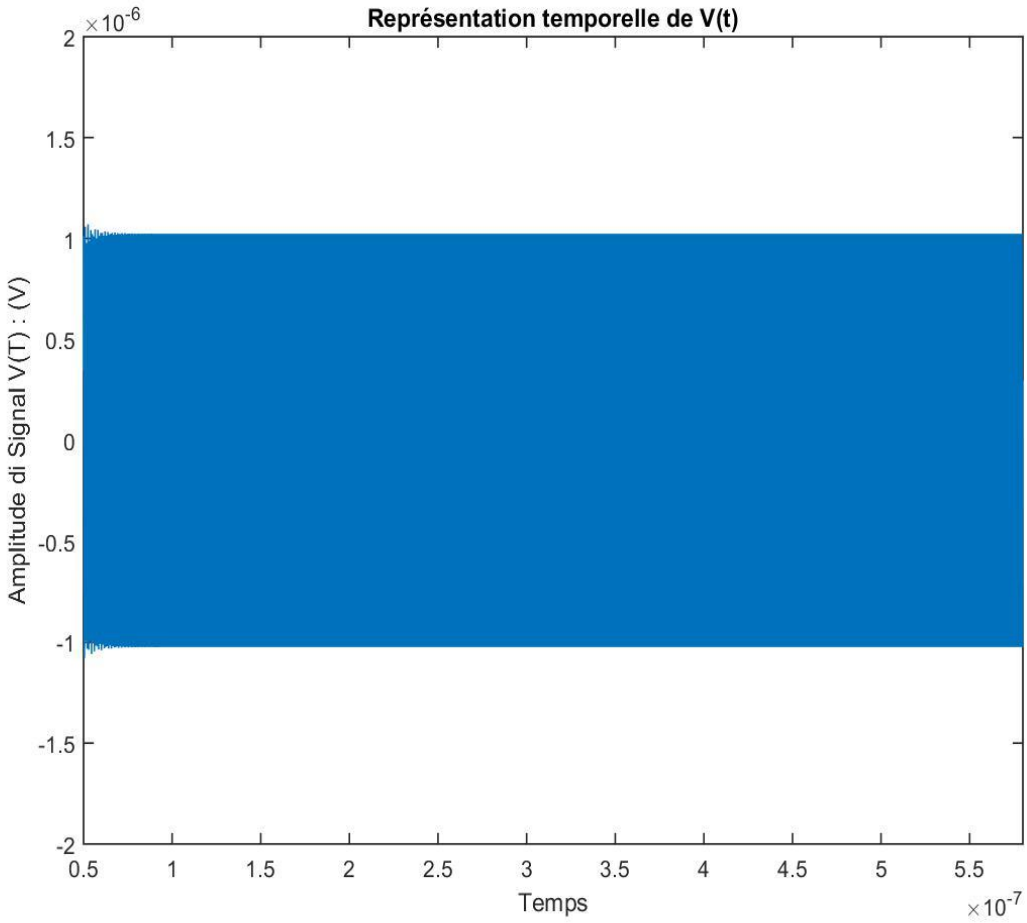

Figure III.8:Représentation temporelle du signal V(t).

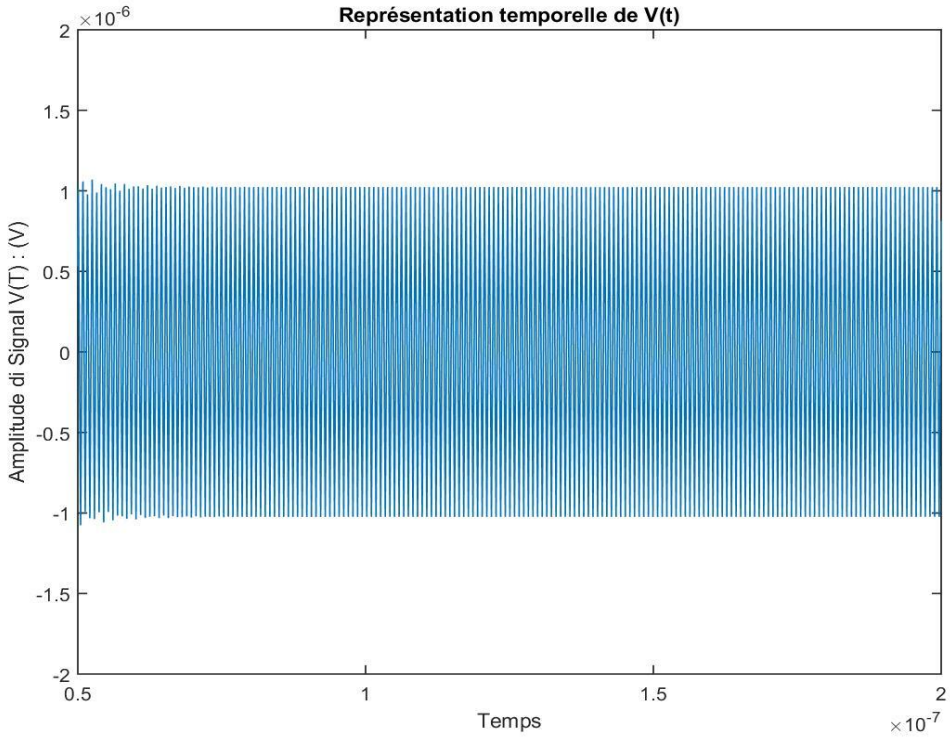

Figure III.9:Zoom sur la représentation temporelle du signal V(t)

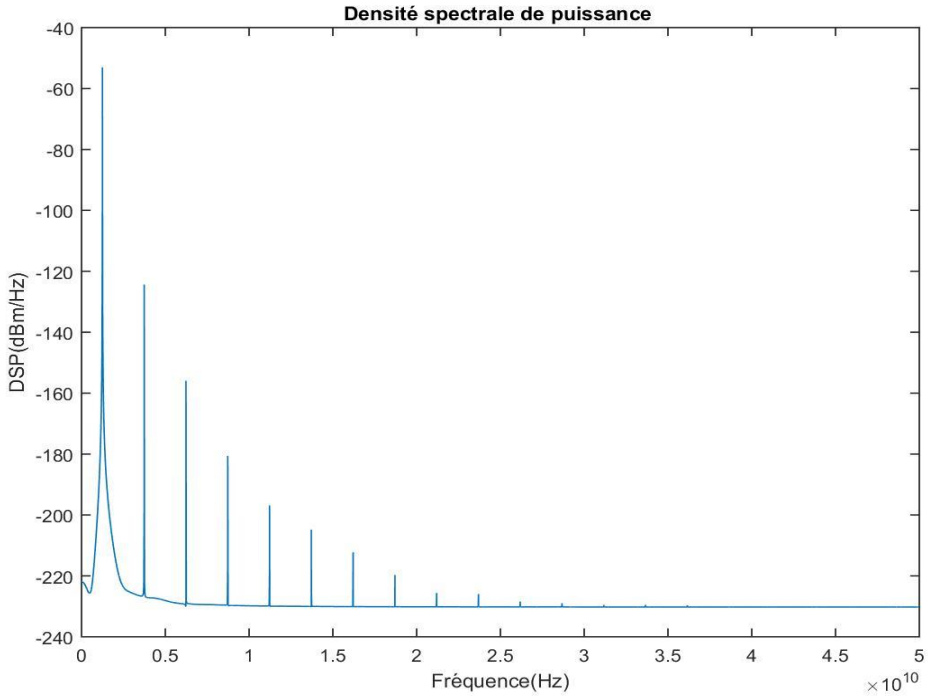

Figure III.10:Représentation de la densité spectrale de puissance du signal V(t).

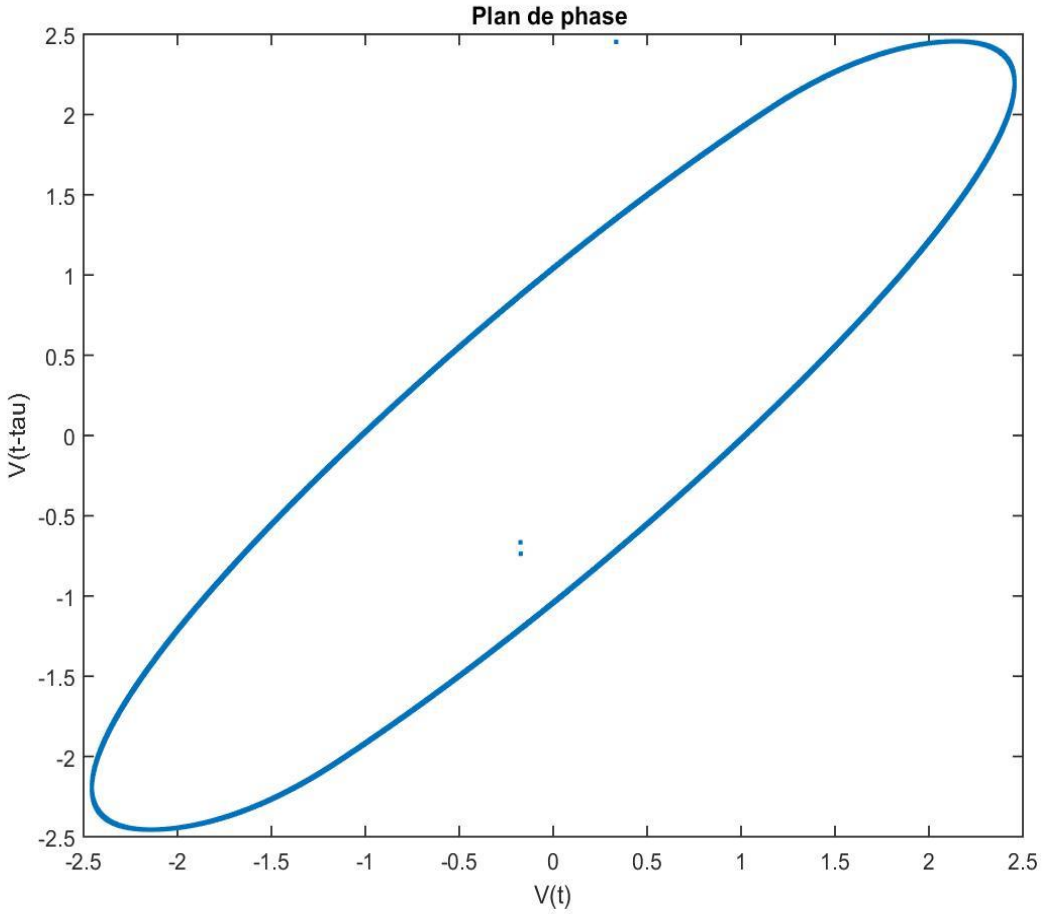

Figure III.11:Plan de phase.

3. Etude pour $\boldsymbol{\beta_{12} = \beta_{22} = 0.07}$ et$\boldsymbol{\beta_{11} = \beta_{21} = 0.08}$

Dans la figure III.12, on remarque que le signal est de nature quasi-périodique.

Ensuite dans la figure III.13, le spectre présente une structure composée de plusieurs fréquences de base accompagnées de leurs multiples harmoniques.

On met en évidence la présence d'un attracteur de type tore, caractéristique d'un régime quasi-périodique. Figure III.14

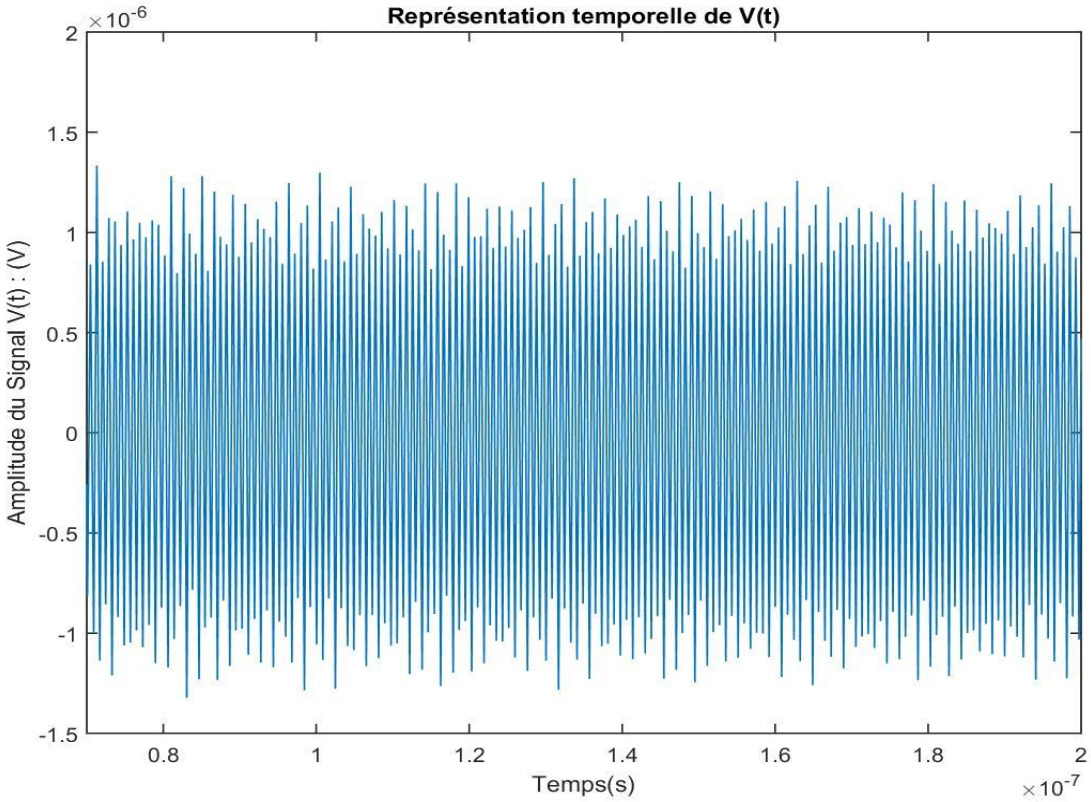

Figure III.12:Représentation temporelle du signal V(t).

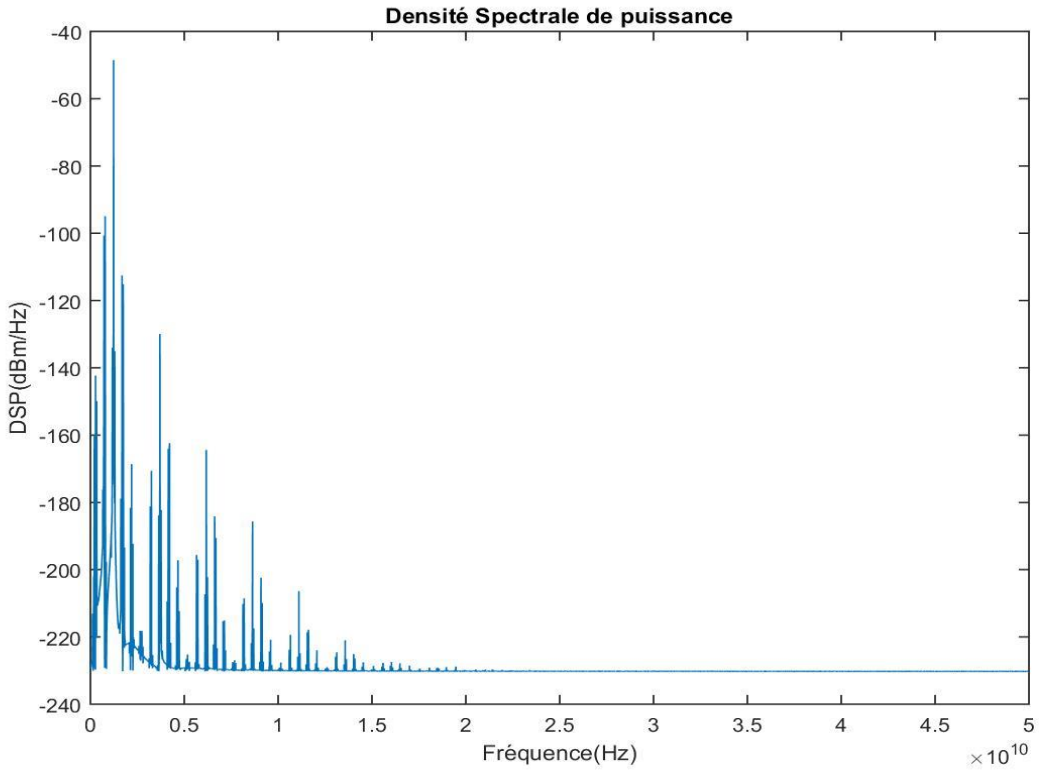

Figure III.13:Représentation de la densité spectrale de puissance du signal V(t).

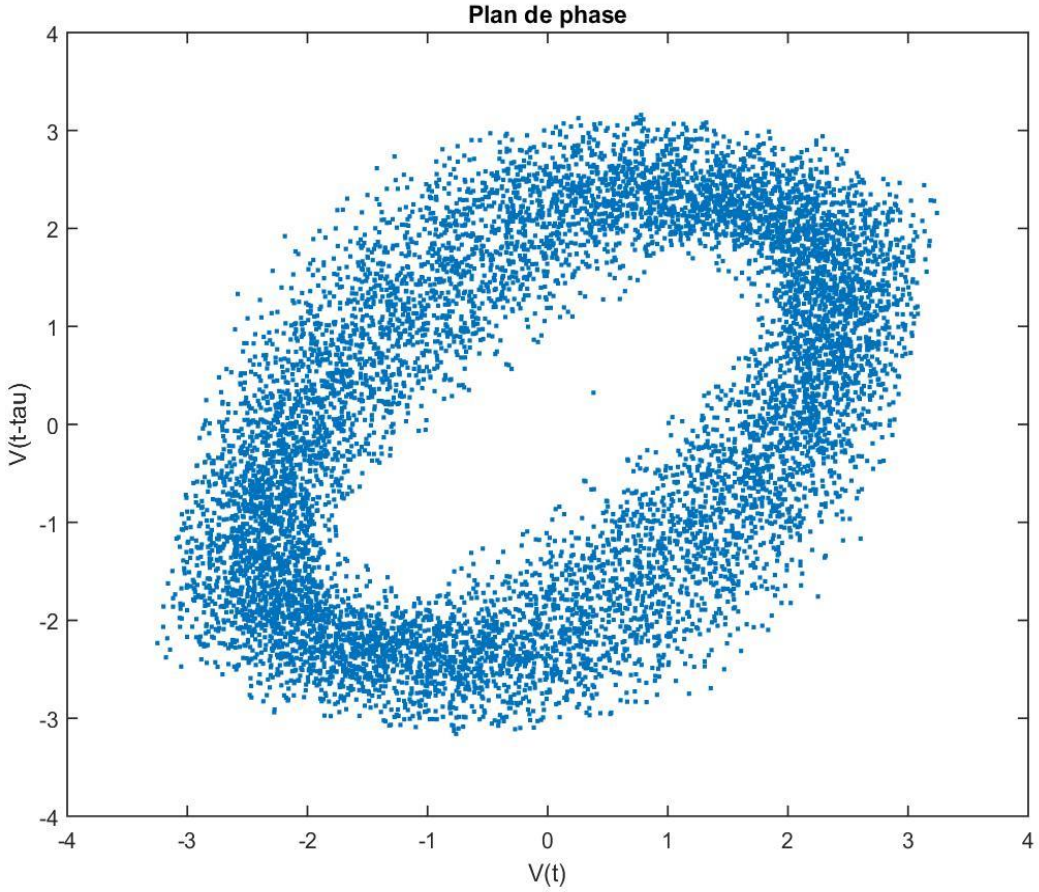

Figure III.14:Plan de phase.

4. Etude pour $\boldsymbol{\beta_{11} = \beta_{21} = 0.1}$ Et $\boldsymbol{\beta_{12} = \beta_{22} = 0.09}$

Le signal se caractérise ici par une évolution chaotique, non prévisible et sensible aux conditions initiales. Figure III.15 et figure III.16

La densité spectrale de puissance, caractérisée par un spectre dense, confirme le caractère chaotique du signal. Figure III.17

L'attracteur observé présente les caractéristiques d'un attracteur étrange. Figure III.18

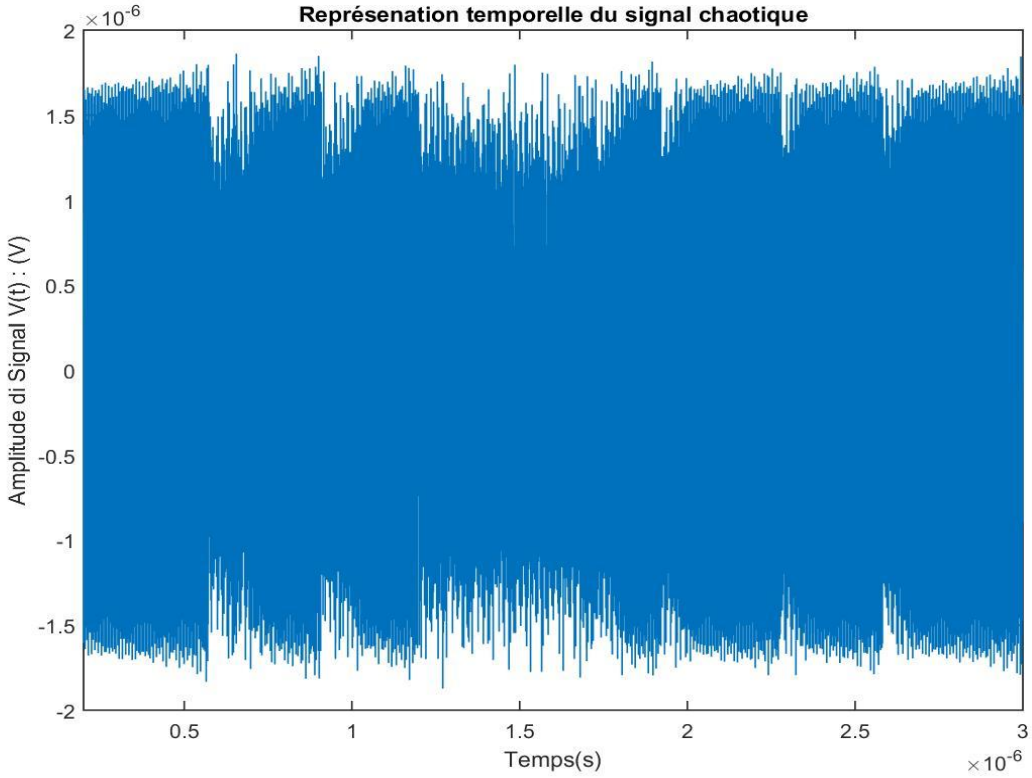

Figure III.15:Représentation temporelle du signal V(t).

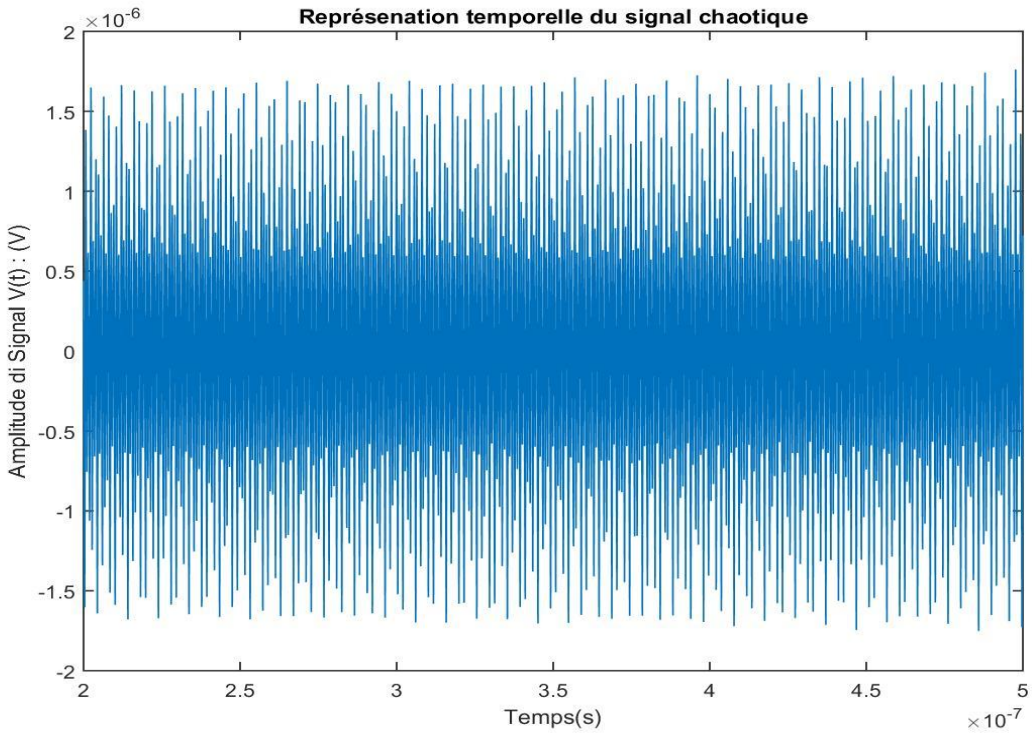

Figure III.16:Zoom sur la représentation temporelle du signal V(t).

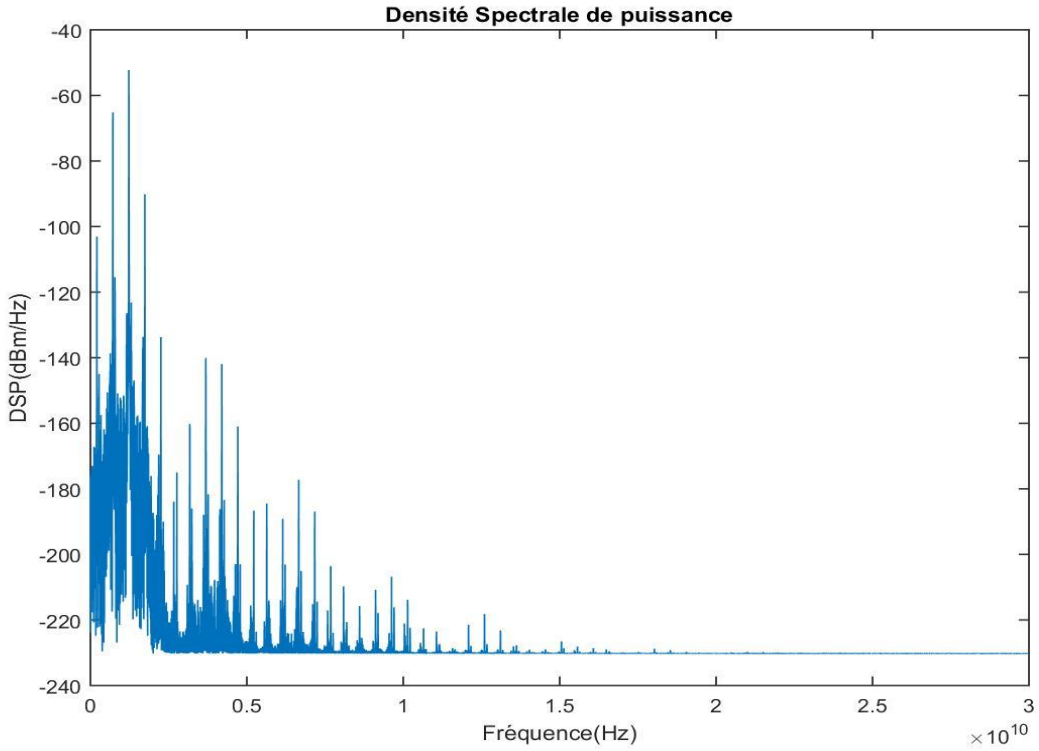

Figure III.17:Représentation de la densité spectrale de puissance du signal V(t).

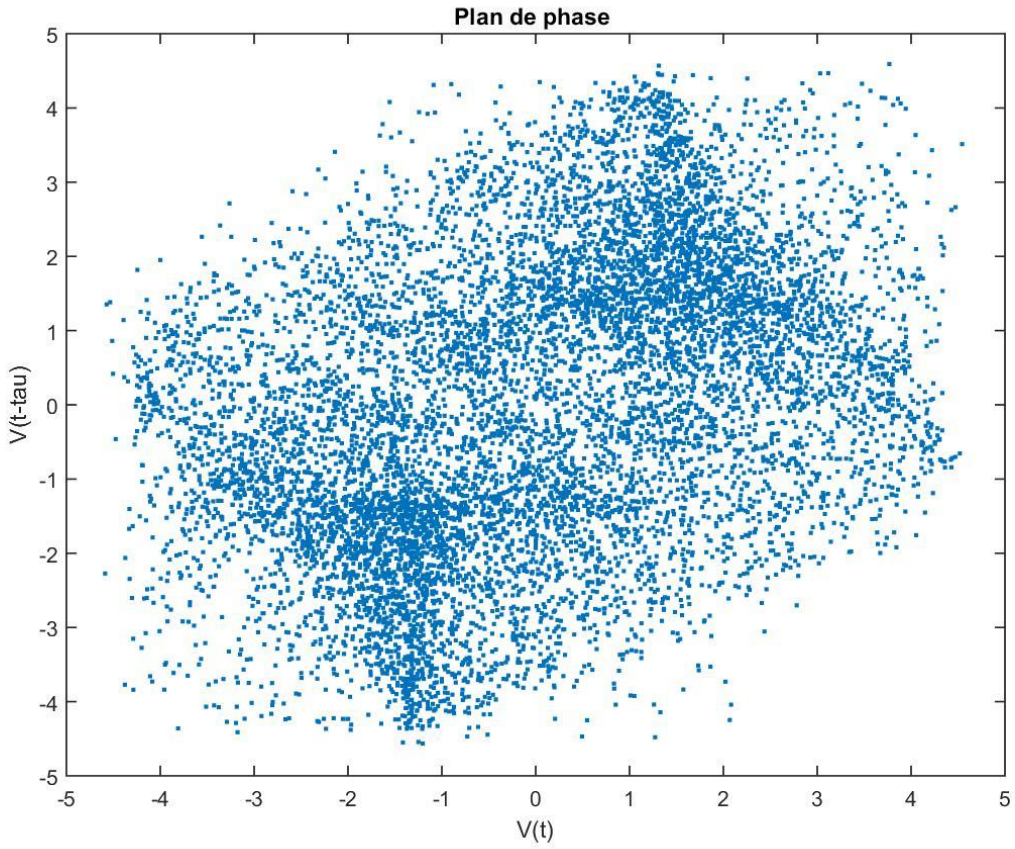

Figure III.18:Plan de phase.

III.5.1 Chiffrement et déchiffrement avec OptiSystem

Comme mentionné précédemment, les opérations de chiffrement et de déchiffrement ont été réalisées à l'aide du logiciel OptiSystem. Le même fichier.dat, contenant le signal chaotique préalablement généré sous MATLAB, a été utilisé à la fois pour le chiffrement et le déchiffrement.

Le signal chaotique est appliqué à l'entrée d'un modulateur Mach-Zehnder (MZM), puis combiné optiquement au signal optique modulé par le message d'information, comme illustré dans les figures III.19, III.20, III.21. Le signal optique ainsi chiffré (figure III.22) est ensuite dirigé vers une photodiode pour être converti en signal électrique.

Du côté du récepteur, le signal chaotique répliqué est injecté dans un second MZM, polarisé en opposition de phase par rapport à celui de l'émetteur. Après la détection optoélectronique, les deux signaux sont additionnés, ce qui permet de reconstituer le message original. (figure III.23).

Les résultats obtenus montrent que le chiffrement et le déchiffrement sont effectués avec succès, sous l'hypothèse d'une synchronisation parfaite entre les signaux chaotiques de l'émetteur et du récepteur.

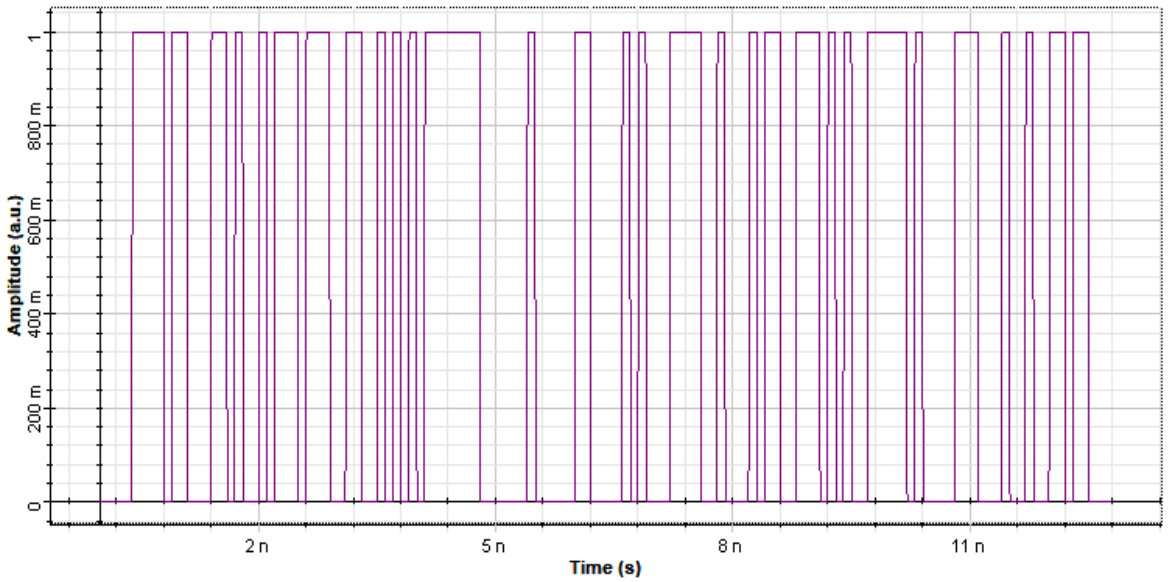

Figure III.19:le message

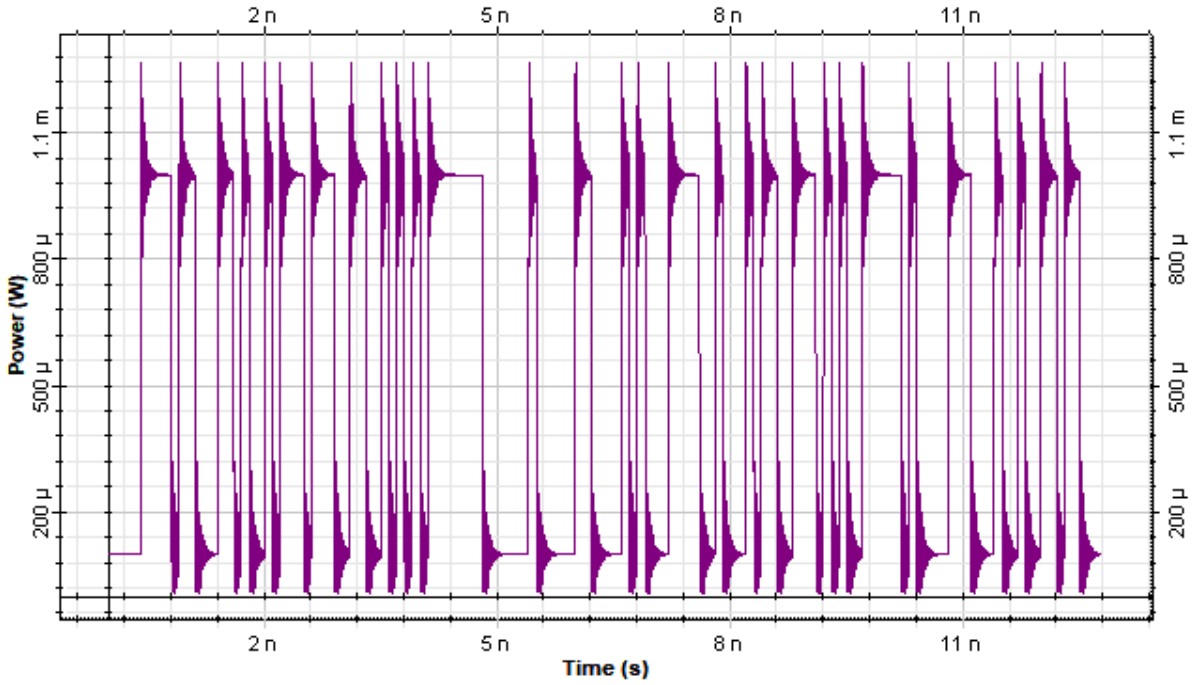

Figure III.20: Le message après la modulation

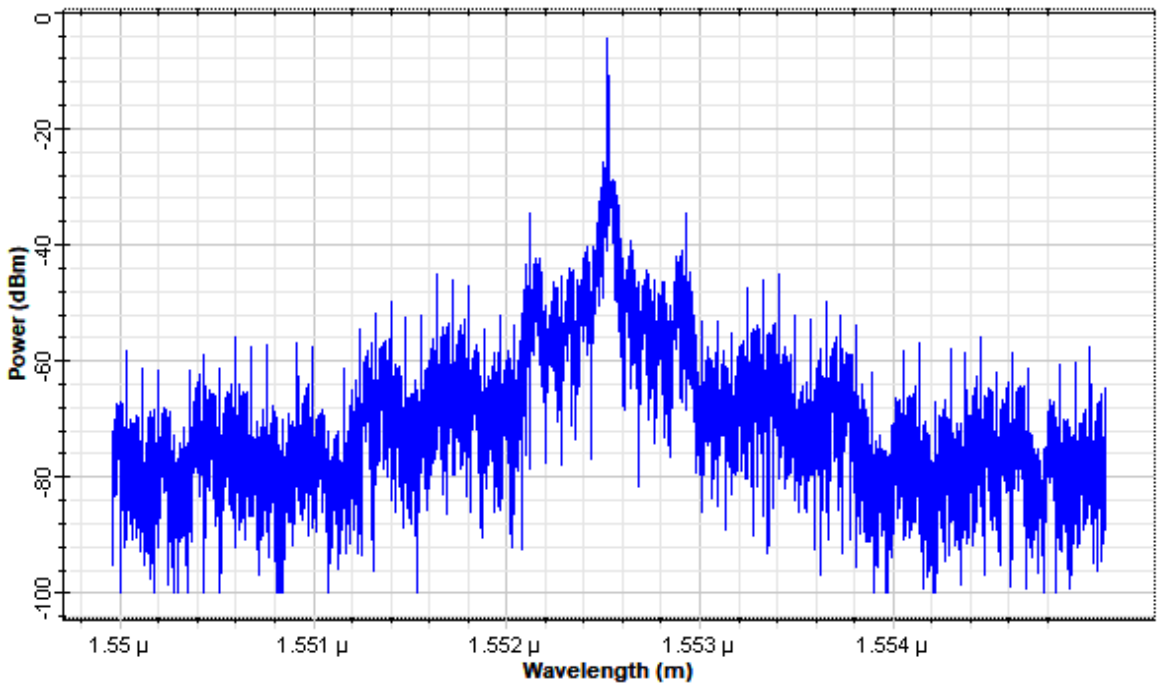

Figure III.21:Le spectre du signal optique modulé

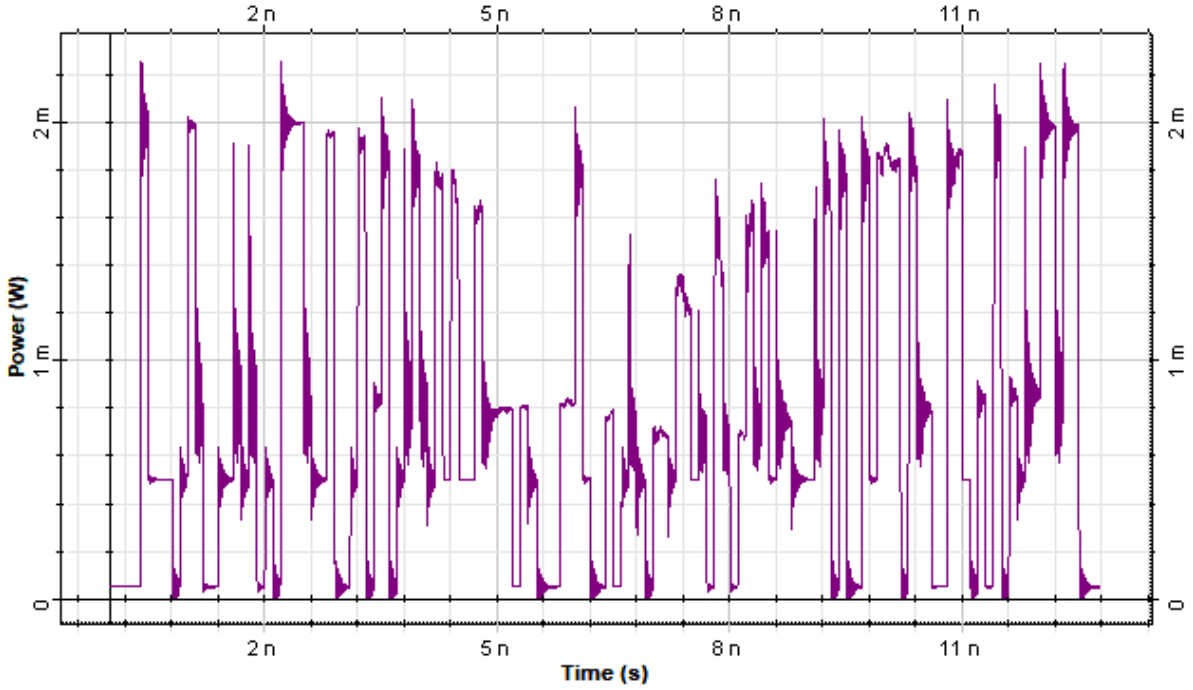

Figure III.22: Le message émis chiffré.

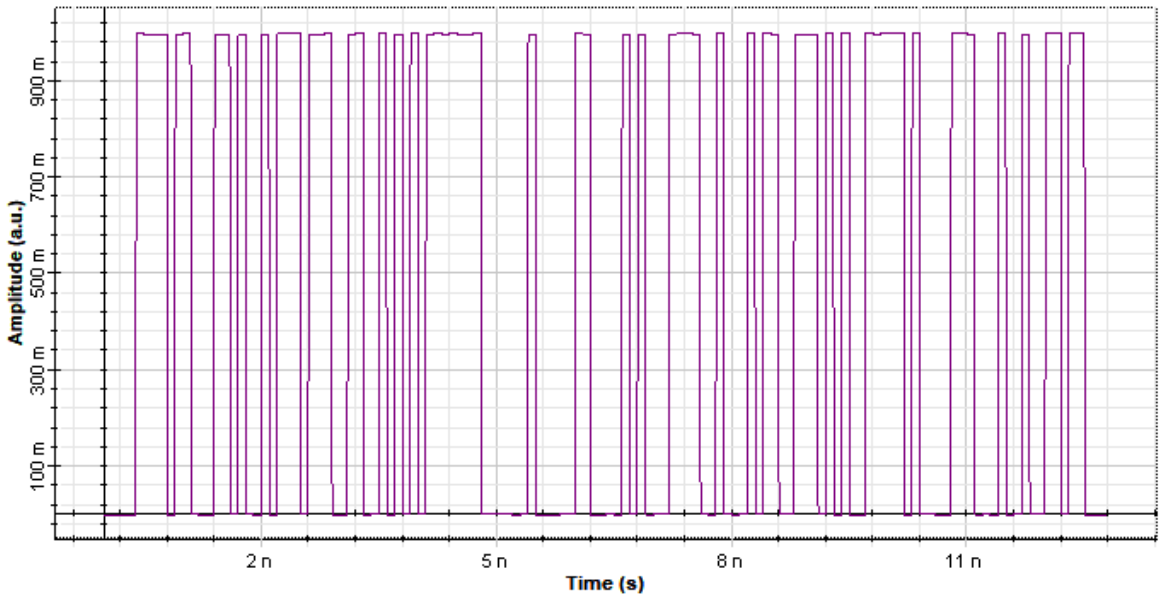

Figure III.23:Le message reçu après déchiffrement

Conclusion Générale

Ce mémoire a exploré la conception et l'analyse d'un crypto-système chaotique à double retard intégrant deux modulateurs Mach-Zehnder (MZM), dans le but de sécuriser les communications optiques à haut débit. L'originalité de cette approche réside dans l'exploitation des propriétés des systèmes chaotiques, tels que leur sensibilité aux conditions initiales et leur imprévisibilité, pour renforcer la confidentialité des transmissions. Le travail s'est articulé en plusieurs chapitres complémentaires, chacun apportant une brique à la compréhension et à la validation du système proposé.

Nous avons dans un premier temps présenté les fondements des systèmes dynamiques chaotiques, cette partie a permis de comprendre les conditions nécessaires à l'apparition du chaos. Une analyse qualitative (à travers l'espace de phase, les attracteurs) et quantitative (exposants de Lyapunov, diagrammes de bifurcation, dimension fractale) a permis de confirmer la nature chaotique du signal généré et la capacité du système à masquer efficacement les données.

Le Chapitre 2 a été consacré les fondements de la cryptographie, distinguant les approches classiques symétriques et asymétriques avant d'analyser en détail les différentes techniques de chiffrement chaotique.

Enfin, dans le Chapitre 3, nous avons évalué les performances du crypto-système basé sur MZM, en simulant l'ensemble de la chaîne de transmission (émetteur, canal, récepteur). Les résultats obtenus à travers les réponses temporelles, diagrammes de bifurcation et plans de phase montrent que ce type de système permet d'assurer une transmission sécurisée, tout en étant compatible avec les exigences de vitesse des réseaux optiques modernes. Malgré ses performances intéressantes, certaines limites subsistent, notamment en présence de bruit ou d'incertitudes sur les paramètres du système.

Bien que ce type de crypto-système chaotique à double retard basé sur des modulateurs Mach-Zehnder ne soit pas encore commercialisé, les avancées récentes en optoélectronique et en cryptographie chaotique laissent entrevoir une réelle possibilité d'intégration future dans les infrastructures de communication optique à haut débit.

Des perspectives futures pourraient inclure l'implementation matérielle du système ou son extension vers des réseaux de communication plus complexes

Bibliographie

[1] W. Stallings. 7th ed., Pearson, 2017 *Cryptography and Network Security: Principles and Practice*.

[2] L. K. Voon and C. S. Lim. Pearson, 2013 *MATLAB for Engineers*.

[3] Kacimi El Hassani Nour El Houda. (2017), Etude et implémentation FPGA d'un système chaotique Auto commuté [Mémoire de Master]. Université SAAD DAHLAB de BLIDA.

[4] Strogatz, S. H. (2018). *Nonlinear dynamics and chaos: With applications to physics, biology, chemistry, and engineering* (2nd ed.). CRC Press.

[5] Filali, H., &Chouchane, K. (2020). *Sur un algorithme pour le calcul des exposants de Lyapunov d'un système dynamique* [Mémoire de master, Centre universitaire AbdelhafidBoussouf - Mila].

[6] Benamor, A. 2021 . Systèmes linéaires commande . Université Badji Mokhtar Annaba, Algérie.

[7] Boulekroune, H. (2020). *Observation et analyse du comportement dynamique dans un circuit chaotique basé sur un memristor* [Mémoire de master, Centre Universitaire Abdelhafid Boussouf – Mila].

[8] Boukheche, D., & Boulemdaoud, A. (2021/2022). *Systèmes dynamiques non linéaires* (Mémoire de fin d'études, Centre Universitaire AbdElhafidBoussouf – Mila).

[9] Bendaoud, M. (2019). *Étude et conception d'un système chaotique basé sur l'oscillateur Colpitts pour les communications sécurisées* [Mémoire de master, Université de Tlemcen].

[10] Kharkhache, C., &Chaibi, S. (2019). *Le chaos dans les systèmes dynamiques* (Mémoire de fin d'études, Université Larbi Tébessi – Tébessa).

[11] Benhabib, C. (2014). *Étude d'un système chaotique pour la sécurisation des communications optiques* (Mémoire de master, Université de Tlemcen, Faculté de Technologie.

[12] BendibIslem. (2020), CAPACité de «DEEP LEARNING»A prédire les CHAOS DANS un système Chaotique [Mémoire de Master]. Université Larbi Tébessi – Tébessa

[13] Azib, D. B. (2010). *Systèmes chaotiques et hyperchaotiques pour la transmission sécurisée de données* [Mémoire de magister, Faculté des Sciences de l'Ingénieur, Laboratoire de Télécommunications, Université de Tlemcen].

[14] Bouchanine, H., & Guermache, O. (2021). *Étude de la dynamique et chaotique du système de Lorenz* [Mémoire de magister, Université Abdelhafid Boussouf – Mila].

[15] Gasri, A. (2018). *Chaos et synchronisation généralisée dans les systèmes dynamiques* (Mémoire de fin d'études, Université Frères Mentouri – Constantine 1).

[16] Moussaoui, L., &Chouaichia, S. (2023). *Étude et simulation d'un crypto-système basé sur l'algorithme AES-GCM : Application au cryptage des images médicales* [Mémoire de master, Université 8 Mai 1945 – Guelma].

[17] Amokrane, M., &Dahmouni, L. (2018). *Étude et implémentation d'algorithmes de chiffrement à clé secrète et à clé publique : Application au cryptage de la parole* [Mémoire de master, Université Mouloud Mammeri – Tizi Ouzou, Faculté de Génie Électrique et d'Informatique].

[18] Bouhous, A. (2018). *Sécurisation de l'information via un canal optique* [Thèse de doctorat, Université Mohamed Seddik Ben Yahia, Faculté des Sciences et de la Technologie, Département d'électronique].

[19] Malica, T., Bouchez, G., Wolfersberger, D. et al. High-frequency chaotic bursts in laser diode with optical-feedback. Commun Phys 5, 287 (2022). https://doi.org/10.1038/s42005-022-01052-5 . Date d'accès 12/03/2025

[20] RP Photonics. (n.d.). *Electro-optic modulators – EOM, Pockels cells.* https://www.rp-photonics.com/electro_optic_modulators.html . Date d'accès 20/03/2025

[21] Newport. (n.d.). *Practical uses and applications of electro-optic modulators* . https://www.newport.com . Date d'accès 23/03/2025

[22] Bennia, S., & Haddad, A. (2017). *Étude et simulation de l'interféromètre Mach-Zehnder en vue d'une application comme biocapteur* [Mémoire de master, Mention Électronique, Spécialité Micro Opto Électronique].

[23] Pisarchik, A. N., & Zanin, M. (2011). Chaotic map cryptography: A survey. International Journal of Computer Science and Network Security, 11(5), 1–6.

[24] Kanyiki, T. (2018). *Apport de la méthode de Runge-Kutta d'ordre 4 dans la dynamique de système mécanique*. ISTE OpenScience